(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2004年6月3日 (03.06.2004)

PCT

(10) 国際公開番号
WO 2004/046936 A1

(51) 国際特許分類[7]: G06F 12/14, G09C 1/00, G11B 20/10

(21) 国際出願番号: PCT/JP2003/013752

(22) 国際出願日: 2003年10月28日 (28.10.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-336754
2002年11月20日 (20.11.2002) JP

(71) 出願人 (米国を除く全ての指定国について): ソニー株式会社 (SONY CORPORATION) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 Tokyo (JP).

(72) 発明者; および

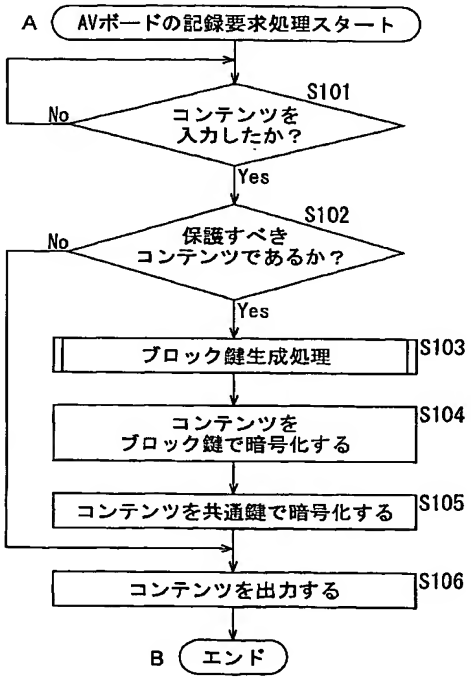
(75) 発明者/出願人 (米国についてのみ): 千秋 進 (SENSHU,Susumu) [JP/JP]; 〒141-0001 東京都 品川区 北品川６丁目７番３５号 ソニー株式会社内 Tokyo (JP).

(74) 代理人: 稲本 義雄 (INAMOTO,Yoshio); 〒160-0023 東京都 新宿区 西新宿７丁目１１番１８号 ７１１ビルディング４階 Tokyo (JP).

[続葉有]

(54) Title: RECORDING SYSTEM AND METHOD, RECORDING DEVICE AND METHOD, INPUT DEVICE AND METHOD, REPRODUCTION SYSTEM AND METHOD, REPRODUCTION DEVICE AND METHOD, RECORDING MEDIUM, AND PROGRAM

(54) 発明の名称: 記録システムおよび方法、記録装置および方法、入力装置および方法、再生システムおよび方法、再生装置および方法、記録媒体、並びにプログラム



A...START OF AV BOARD RECORDING REQUEST PROCESSING
S101...CONTENT RECEIVED?
S102...CONTENT TO BE PROTECTED?
S103...BLOCK KEY GENERATION PROCESSING
S104...ENCRYPT CONTENT WITH BLOCK KEY
S105...ENCRYPT CONTENT WITH COMMON KEY
S106...OUTPUT CONTENT
B...END

(57) Abstract: A recording system and method, a recording device and method, an input device and method, a reproduction system and method, a reproduction device and method, a recording medium, and a program for protecting a content flexibly based on whether or not the content must be protected. When a mutual authentication unit (121) has already performed mutual authentication with an AV board (112) and a content received by the mutual authentication unit (121) has been encrypted with a common key, an input/output controller (122) judges that a content received via a bus (113) is to be protected on the bus (113) and, under control of a recording/reproduction processing unit (123), generates protection information "0", which indicates that the content should be protected on the bus (113), and records the generated protection information, as well as the content, on an optical disc (141). The present invention is applicable to an optical disc recording/reproduction device.

(57) 要約: 保護の要不要に基づいて、コンテンツを柔軟に保護することができるようにした記録システムおよび方法、記録装置および方法、入力装置および方法、再生システムおよび方法、再生装置および方法、記録媒体、並びにプログラムに関する。入出力制御部１２２は、相互認証部１２１によりＡＶボード１１２との間で相互認証がされ、かつ、相互認証部１２１に入力されたコンテンツが共通鍵で暗号化されている場合、バス１１３を介して入力されるコンテンツがバス１１３上で保護されるべきコンテンツであると判断し、記録再生処理部１２３を制御し、バス１１３上で保護すべきコンテンツであるという保護情報「０」を生成させ、生成された保護情報を、コンテンツとともに、光ディスク１４１に記録させる。本発明は、光ディスク記録再生装置に適用できる。

WO 2004/046936 A1

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

明細書

記録システムおよび方法、記録装置および方法、入力装置および方法、再生システムおよび方法、再生装置および方法、記録媒体、並びにプログラム

技術分野

本発明は、記録システムおよび方法、記録装置および方法、入力装置および方法、再生システムおよび方法、再生装置および方法、記録媒体、並びにプログラムに関し、特に、保護の要不要に基づいて、コンテンツを柔軟に保護することができるようにした記録システムおよび方法、記録装置および方法、入力装置および方法、再生システムおよび方法、再生装置および方法、記録媒体、並びにプログラムに関する。

背景技術

記録再生装置（例えば、CD-RW ドライブなど）においては、ディスクに記録または再生を行う場合、コンテンツを保護するために、正当な記録再生制御と不正コピーの防止が求められている。

例えば、特表２００２－５２１７８９号公報には、ユーザデータとユーザコントロールデータにより構成されるデータフォーマットを用いて、ディスクに記録または再生を行うことが提案されている。

このようなデータフォーマットにおいては、そのユーザデータ部分に、ディスクに固有のＩＤであるディスクＩＤを作用させた鍵で暗号化して記録することによりコンテンツが不当なコピーから保護される。

また、特開２００２－８４２７１号公報には、図１に示される記録再生装置１が開示されている。

図１の例においては、記録再生装置１は、ドライブ１１、ＡＶボード１２および専用バス１３により構成される。ドライブ１１は、記録再生処理部２１を有し、ＡＶボード１２は、ＡＶコンテンツ処理部３１、コンテンツ保護部３２、入力部

３３および出力部３４を有している。

記録再生処理部２１は、光ディスク４１が装着されると、光ディスク４１に固有のディスクＩＤおよびＲＫＢ（Renewal Key Block）を取得し、専用バス１３を介して、ＡＶボード１２のコンテンツ保護部３２に供給する。コンテンツ保護部３２は、取得したディスクＩＤおよびＲＫＢから得たディスク鍵を作用させた鍵を生成し、記憶する。

ＡＶコンテンツ処理部３１は、アンテナなどにより構成される入力部３３を介して受信された著作権を保護する必要があるコンテンツを、コンテンツ保護部３２に供給する。コンテンツ保護部３２は、予め記憶されているディスクＩＤおよびＲＫＢから得たディスク鍵などを作用させた鍵でコンテンツを暗号化し、保護すべきコンテンツとして、専用バス１３を介して、記録再生処理部２１に供給する。記録再生処理部２１は、暗号化されたコンテンツを受信し、光ディスク４１に記録する。

また、記録再生処理部２１は、光ディスク４１から所定の暗号化されたコンテンツを再生し、専用バス１３を介して、コンテンツ保護部３２に供給する。コンテンツ保護部３２は、暗号化されたコンテンツを、ディスクＩＤおよびＲＫＢから得たディスク鍵を作用させた鍵で復号し、ＡＶコンテンツ処理部３１に供給する。ＡＶコンテンツ処理部３１は、復号されたコンテンツを、例えば、MPEG（Moving Picture Experts Group）方式でデコードし、再生する。出力部３４は、再生されたコンテンツを出力する。

以上のように、ドライブ１１とＡＶボード１２間においては、記録再生装置１内の専用バス１３を介しているため、外部からアクセスされることはなく、ディスクＩＤまたはＲＫＢを利用して、コンテンツを保護することができる。

図１の変形例として、図２に示されるような、記録再生装置５１が考えられる。尚、図２において、図１における場合と対応する部分には対応する符号を付してあり、その説明は繰り返しになるので省略するが、図２の例の場合、ドライブ１１とＡＶボード１２がバス６１（汎用バス）を介して分離されている（例えば、

家庭内ＬＡＮ(Local Area Network)などで分離されている）。

したがって、図２の例においては、バス６１にディスクＩＤおよびＲＫＢがそのまま流れてしまうため、これらが盗用される危険が生じる。例えば、コンテンツを記録する場合、ＨＤＤ(Hard Disk Drive)７１をバス６１に接続することにより、バス６１上にある「ディスクＩＤ」、「ＲＫＢ」および「ディスクＩＤおよびＲＫＢから得たディスク鍵を用いて暗号化されたコンテンツ」が吸い上げられ（モニターされ）、ＨＤＤ７１にコピーされてしまう。

図２の例の場合、ＨＤＤ７１には、以上のようにして吸い上げられた、１６ＢのディスクＩＤ、数ＭＢのＲＫＢ、および２０ＧＢの暗号化コンテンツ、並びに、数ＫＢのプログラムが記憶されている。ＨＤＤ７１により、これらの「ディスクＩＤ」、「ＲＫＢ」および「ディスクＩＤおよびＲＫＢから得たディスク鍵を用いて暗号化されたコンテンツ」が、ＡＶボード１２に与えられると、ＡＶボード１２は、正当な光ディスク４１から再生されたものとの識別ができないため、コンテンツを再生してしまう。

以上のように、吸い上げた「ディスクＩＤ」、「ＲＫＢ」および「ディスクＩＤおよびＲＫＢから得たディスク鍵を用いて暗号化されたコンテンツ」を、ＡＶボード１２に対して与える「なりすましドライブ」または「なりすましプログラム」は、再生実行型装置またはプログラムとして、一般的に流通されてしまう恐れがある。

したがって、ドライブ１１とＡＶボード１２が、バス６１を介して分離している構成の記録再生装置５１においては、正当なディスクでなくても、ＨＤＤ７１のように、何らかのメディアにコピーされ、流通されてしまう恐れがある。

そこで、図３に示されるような相互認証を行う記録再生装置８１が提案される。図３の例においては、ドライブ１１に相互認証部９１が設けられ、ＡＶボード１２に相互認証部９２が設けられ、それらの間で相互認証処理が実行されることにより共有された共通鍵を用いて暗号化することで、コンテンツの送受信が行われる。

これにより、記録再生装置１または記録再生装置５１で記録された光ディスクと互換性があり、かつ、相互認証機能を有しないＨＤＤ７１においては、「ディスクＩＤ」、「ＲＫＢ」および「ディスクＩＤおよびＲＫＢから得たディスク鍵を用いて暗号化されたコンテンツ」がコピーされたとしても、その復号ができないので、実質的にコピーを不可能にすることができる。したがって、上述した「なりすましドライブ」または「なりすましプログラム」を防止することができる。

しかしながら、最近、暗号化コンテンツをフリーで提供するという超流通用途のため、あるいは、ＰＣ(Personal Computer)ストレージ用途のために、保護する必要がないコンテンツは、ユーザから見てコピー可能なように、バス１３上では暗号化せずに記録、再生できるようにし、かつ、保護すべきコンテンツは、実質的にコピー防止できるようにすることが望まれている。

しかしながら、現在、一般のＰＣのＨＤＤ７１には、相互認証処理を実行する機能が備えられていないため、記録再生装置８１においては、ＨＤＤ７１には、保護すべき特定のコンテンツだけでなく、ＰＣストレージ用途のための保護不要のコンテンツまでもコピーすることができなくなってしまうといった課題があった。

発明の開示

本発明はこのような状況に鑑みてなされたものであり、保護の要不要に基づいて、コンテンツを柔軟に保護することができるようにするものである。

本発明の記録システムは、入力装置は、入力されたコンテンツを保護するか否かを判断する判断手段を備え、記録装置は、判断手段により判断された結果に基づいて、コンテンツがバス上での伝送において保護すべきコンテンツであるか否かを示す保護情報を、コンテンツとともに記録媒体に記録する記録手段を備えることを特徴とする。

記録手段は、コンテンツの所定の単位ごとに保護情報を記録するようにするこ

とができる。

所定の単位は、２０４８バイトであるようにすることができる。

記録装置は、判断手段によりコンテンツを保護すると判断された場合、記録媒体のＩＤと記録媒体鍵を作用させてコンテンツを暗号化する暗号化手段をさらに備えるようにすることができる。

記録装置は、判断手段によりコンテンツを保護しないと判断された場合、少なくとも、記録媒体の記録媒体鍵を作用させてコンテンツを暗号化する暗号化手段をさらに備えるようにすることができる。

入力装置および記録装置は、それぞれ相互に認証する認証手段をさらに備えるようにすることができる。

入力装置は、判断手段によりコンテンツを保護すると判断された場合、バスへのコンテンツの送出前に、コンテンツを暗号化する第１の暗号化手段をさらに備え、記録装置は、判断手段によりコンテンツを保護すると判断された場合、記録手段によるコンテンツの記録前に、コンテンツを暗号化する第２の暗号化手段をさらに備えるようにすることができる。

判断手段によりコンテンツを保護しないと判断された場合、第１の暗号化手段は、バスへのコンテンツの送出前に、コンテンツを暗号化することを禁止するようにすることができる。

本発明の第１の記録方法は、入力装置は、入力されたコンテンツを保護するか否かを判断し、記録装置は、判断された結果に基づいて、コンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を、コンテンツとともに記録媒体に記録することを特徴とする。

本発明の記録装置は、バスを介して接続された他の装置と相互に認証を行う認証手段と、他の装置からバスを介して供給される第１の暗号化方法により暗号化されたコンテンツを復号する復号手段と、復号手段により復号されたコンテンツとともに、バス上での伝送において保護すべきコンテンツであることを示す保護情報を、記録媒体に記録する記録手段とを備えることを特徴とする。

復号されたコンテンツを、第２の暗号化方法により暗号化する暗号化手段をさらに備えるようにすることができる。

暗号化手段は、記録媒体のＩＤと記録媒体鍵を作用させて復号されたコンテンツを暗号化するようにすることができる。

記録手段は、他の装置からバスを介して供給されたコンテンツが、第１の暗号方法により暗号化されていないコンテンツの場合、コンテンツを、バス上での伝送において保護すべきコンテンツでないことを示す保護情報とともに記録するようにすることができる。

本発明の第２の記録方法は、バスを介して接続された他の装置と相互に認証を行う認証ステップと、他の装置からバスを介して供給される暗号化されたコンテンツを復号する復号ステップと、復号ステップの処理により復号されたコンテンツとともに、バス上での伝送において保護すべきコンテンツであることを示す保護情報を、記録媒体に記録する記録ステップとを含むことを特徴とする。

本発明の第１の記録媒体のプログラムは、バスを介して接続された他の装置と相互に認証を行う認証ステップと、他の装置からバスを介して供給される暗号化されたコンテンツを復号する復号ステップと、復号ステップの処理により復号されたコンテンツとともに、バス上での伝送において保護すべきコンテンツであることを示す保護情報を、記録媒体に記録する記録ステップとを含むことを特徴とする。

本発明の第１のプログラムは、バスを介して接続された他の装置と相互に認証を行う認証ステップと、他の装置からバスを介して供給される暗号化されたコンテンツを復号する復号ステップと、復号ステップの処理により復号されたコンテンツとともに、バス上での伝送において保護すべきコンテンツであることを示す保護情報を、記録媒体に記録する記録ステップとを含むことを特徴とする。

本発明の入力装置は、バスを介して接続された記録装置と相互に認証を行う認証手段と、入力されたコンテンツがバス上での伝送において保護すべきコンテンツであるか否かに応じて、コンテンツを第１の暗号化方法で暗号化する第１の暗

号化手段と、第１の暗号化手段により暗号化されたコンテンツを、バスを介して記録装置に供給する供給手段とを備えることを特徴とする。

第１の暗号化手段により暗号化されたコンテンツを、第２の暗号化方法で暗号化する第２の暗号化手段をさらに備えるようにすることができる。

第１の暗号化手段および第２の暗号化手段のうちの一方は、記録媒体のＩＤと記録媒体鍵を作用させてコンテンツを暗号化するようにすることができる。

本発明の入力方法は、バスを介して接続された記録装置と相互に認証を行う認証ステップと、入力されたコンテンツがバス上での伝送において保護すべきコンテンツであるか否かに応じて、コンテンツを暗号化する暗号化ステップと、暗号化ステップの処理により暗号化されたコンテンツを、バスを介して記録装置に供給する供給ステップとを含むことを特徴とする。

本発明の第２の記録媒体のプログラムは、バスを介して接続された記録装置と相互に認証を行う認証ステップと、入力されたコンテンツがバス上での伝送において保護すべきコンテンツであるか否かに応じて、コンテンツを暗号化する暗号化ステップと、暗号化ステップの処理により暗号化されたコンテンツを、バスを介して記録装置に供給する供給ステップとを含むことを特徴とする。

本発明の第２のプログラムは、バスを介して接続された記録装置と相互に認証を行う認証ステップと、入力されたコンテンツがバス上での伝送において保護すべきコンテンツであるか否かに応じて、コンテンツを暗号化する暗号化ステップと、暗号化ステップの処理により暗号化されたコンテンツを、バスを介して記録装置に供給する供給ステップとを含むことを特徴とする。

本発明の再生システムは、再生装置は、記録媒体からコンテンツ、およびコンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生手段と、再生手段により再生された保護情報に基づいて、バス上の出力装置へのコンテンツの送出を制御する送出制御手段とを備え、出力装置は、送出制御手段により送出されたコンテンツを外部に出力する出力手段を備えることを特徴とする。

保護情報は、コンテンツの所定の単位ごとに記録されているようにすることができる。

所定の単位は、２０４８バイトであるようにすることができる。

再生装置は、再生手段により再生されたコンテンツを復号する復号手段をさらに備えるようにすることができる。

再生装置は、バス上の装置を認証する認証手段をさらに備えるようにすることができる。

再生装置は、保護情報によりコンテンツがバス上の伝送において保護すべきコンテンツであることが示され、かつ、認証手段によりバス上の出力装置が認証されている場合、バスへのコンテンツの送出前に、コンテンツを暗号化する暗号化手段をさらに備え、出力装置は、暗号化手段により暗号化されたコンテンツを復号する第１の復号手段をさらに備えるようにすることができる。

出力装置は、第１の復号手段により復号されたコンテンツを、記録媒体のＩＤと記録媒体鍵を作用させて復号する第２の復号手段をさらに備えるようにすることができる。

保護情報によりコンテンツがバス上の伝送において保護すべきコンテンツであることが示され、かつ、認証手段によりバス上の装置が認証されていない場合、送出制御手段は、バス上の装置へのコンテンツの送出を禁止するようにすることができる。

本発明の第１の再生方法は、再生装置は、記録媒体からコンテンツ、およびコンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生し、再生された保護情報に基づいて、バス上の出力装置へのコンテンツの送出を制御し、出力装置は、再生装置から送出されたコンテンツを外部に出力することを特徴とする。

本発明の再生装置は、記録媒体からコンテンツ、およびコンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生手段と、再生手段により再生された保護情報に基づいて、バスを介しての他の装

置へのコンテンツの出力を制御する出力制御手段とを備えることを特徴とする。

保護情報は、コンテンツの所定の単位ごとに記録されているようにすることができる。

所定の単位は、２０４８バイトであるようにすることができる。

他の装置を認証する認証手段と、コンテンツを暗号化する暗号化手段とをさらに備え、保護情報によりコンテンツがバス上の伝送において保護すべきコンテンツであることが示され、かつ、認証手段により他の装置が認証されている場合、暗号化手段は、バスへのコンテンツの送出前に、コンテンツを暗号化するようにすることができる。

保護情報によりコンテンツがバス上の伝送において保護すべきコンテンツであることが示され、かつ、認証手段により他の装置が認証されていない場合、出力制御手段は、バスへのコンテンツの出力を禁止するようにすることができる。

本発明の第２の再生方法は、記録媒体からコンテンツ、およびコンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生ステップと、再生ステップの処理により再生された保護情報に基づいて、バスを介しての他の装置へのコンテンツの出力を制御する出力制御ステップとを含むことを特徴とする。

本発明の第３の記録媒体のプログラムは、記録媒体からコンテンツ、およびコンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生ステップと、再生ステップの処理により再生された保護情報に基づいて、バスを介しての他の装置へのコンテンツの出力を制御する出力制御ステップとを含むことを特徴とする。

本発明の第３のプログラムは、記録媒体からコンテンツ、およびコンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生ステップと、再生ステップの処理により再生された保護情報に基づいて、バスを介しての他の装置へのコンテンツの出力を制御する出力制御ステップとを含むことを特徴とする。

第１の本発明においては、入力装置により、入力されたコンテンツを保護するか否かが判断され、判断された結果に基づいて、記録装置により、コンテンツがバス上での伝送において保護すべきコンテンツであるか否かを示す保護情報が、コンテンツとともに記録媒体に記録される。

入力装置は、独立した装置であっても良いし、入力記録装置の入力処理を行うブロックであってもよい。

記録装置は、独立した装置であっても良いし、記録再生装置の記録処理を行うブロックであってもよい。

第２の本発明においては、バスを介して接続された他の装置と相互に認証が行われる。そして、他の装置からバスを介して供給される暗号化されたコンテンツが復号され、復号されたコンテンツとともに、バス上での伝送において保護すべきコンテンツであることを示す保護情報が、記録媒体に記録される。

第３の本発明においては、バスを介して接続された記録装置と相互に認証が行われる。そして、入力されたコンテンツがバス上での伝送において保護すべきコンテンツであるか否かに応じて、コンテンツが暗号化され、暗号化されたコンテンツが、バスを介して記録装置に供給される。

第４の本発明においては、再生装置により、記録媒体からコンテンツ、およびコンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報が再生され、再生された保護情報に基づいて、バス上の出力装置へのコンテンツの送出が制御される。そして、出力装置により、再生装置から送出されたコンテンツが外部に出力される。

再生装置は、独立した装置であっても良いし、記録再生装置の再生処理を行うブロックであってもよい。

出力装置は、独立した装置であっても良いし、再生出力装置の出力処理を行うブロックであってもよい。

第５の本発明においては、記録媒体からコンテンツ、およびコンテンツがバス上の伝送において保護すべきコンテンツであるか否かを示す保護情報が再生され、

再生された保護情報に基づいて、バスを介しての他の装置へのコンテンツの出力が制御される。

図面の簡単な説明

図１は、従来の記録再生装置の構成例を示すブロック図である。

図２は、従来の記録再生装置の他の構成例を示すブロック図である。

図３は、従来の記録再生装置のさらに他の構成例を示すブロック図である。

図４は、本発明を適用した記録再生装置の構成例を示すブロック図である。

図５は、本発明のデーターフォーマットの構成例を示す図である。

図６は、図５のデータフレームの構成例を示す図である。

図７は、図５のスクランブルデータフレームの構成例を示す図である。

図８は、図５のユーザコントロールデータの構成例を示す図である。

図９は、図４のコンテンツ保護部１３２の構成例を示すブロック図である。

図１０は、本発明のディスク鍵について説明するツリー構造図である。

図１１Ａは、本発明のディスク鍵に使用されるＲＫＢの例を説明する図である。

図１１Ｂは、本発明のディスク鍵に使用されるＲＫＢの例を説明する図である。

図１２は、図１１Ａおよび図１１ＢのＲＫＢの使用例を説明する図である。

図１３は、図４のＡＶボードの相互認証処理を説明するフローチャートである。

図１４は、図４のドライブの相互認証処理を説明するフローチャートである。

図１５は、図４のＡＶボードの記録要求処理を説明するフローチャートである。

図１６は、図１５のステップＳ１０３のブロック鍵生成処理を説明するフローチャートである。

図１７は、図１６の処理に対応する図４のドライブのディスク情報再生処理を説明するフローチャートである。

図１８は、図４のドライブの記録処理を説明するフローチャートである。

図１９は、図４のドライブの再生処理を説明するフローチャートである。

図２０は、図４のＡＶボードの再生処理を説明するフローチャートである。

図２１は、図４の記録再生装置の他の構成例を示すブロック図である。

図２２は、図２１のドライブの記録処理を説明するフローチャートである。

図２３は、図２１のドライブの再生処理を説明するフローチャートである。

図２４は、本発明の記録再生装置の他の構成例を示すブロック図である。

図２５は、図２４のコンテンツ保護部４１１の構成例を示すブロック図である。

図２６は、図２４のドライブのブロック鍵生成処理を説明するフローチャートである。

図２７は、図２４のＡＶボードの記録要求処理を説明するフローチャートである。

図２８は、図２４のドライブの記録処理を説明するフローチャートである。

図２９は、図２４のドライブの再生処理を説明するフローチャートである。

図３０は、図２４のＡＶボードの再生処理を説明するフローチャートである。

図３１は、図２４の記録再生装置の他の構成例を示すブロック図である。

図３２は、図３１のドライブの記録処理を説明するフローチャートである。

図３３は、図３１のドライブの再生処理を説明するフローチャートである。

図３４は、本発明の記録再生装置の他の構成例を示すブロック図である。

発明を実施するための最良の形態

以下、図を参照して本発明の実施の形態について説明する。

図４は、本発明を適用した記録再生装置１０１の構成例を表している。家庭内ＬＡＮ(Local Area Network)に代表されるバス１１３には、ドライブ１１１、ＡＶボード１１２、およびＨＤＤ(hard disk drive)１１４が接続されている。なお、ドライブ１１１、ＡＶボード１１２、およびＨＤＤ１１４は、独立に販売されるものであり、ユーザにより、バス１１３に接続されるものである。

この例の場合、ドライブ１１１およびＡＶボード１１２は、それぞれ自分自身の秘密鍵と公開鍵を有している。この公開鍵および秘密鍵の登録は、例えば、メーカにより出荷時に、あらかじめ行なわれている。なお、公開鍵は、図示せぬ認

証局が発行した電子署名の中に記憶される。ドライブ１１１およびＡＶボード１１２の間におけるコンテンツの転送には、例えば、RSAなどの公開鍵暗号化方式が使用される。なお、秘密鍵とそれに対応する公開鍵は、一方の鍵に基づいて生成された暗号文を他方の鍵を用いて復号できる関係にある。

ドライブ１１１は、他の装置（図４の例の場合、ＡＶボード１１２）との相互認証処理を実行する相互認証部１２１、ドライブ１１１の各部の制御を実行する入出力制御部１２２、および、ドライブ１１１に装着された光ディスク１４１に、コンテンツの記録または再生を実行する記録再生処理部１２３により構成される。

ＡＶボード１１２は、他の装置（図４の例の場合、ドライブ１１１）との相互認証処理を実行する相互認証部１３１、光ディスク１４１に記憶するコンテンツを暗号化するコンテンツ保護部１３２、アンテナなどにより構成される入力部１３４を介してコンテンツを受信したり、コンテンツをデコードし、出力部１３５に出力するＡＶコンテンツ処理部１３３により構成される。

ドライブ１１１の相互認証部１２１は、ＡＶボード１１２の相互認証部１３１との間で相互認証処理を実行する。具体的に説明すると、ドライブ１１１とＡＶボード１１２が接続され、それぞれの電源がオンされたとき、ＡＶボード１１２の相互認証部１３１は、内蔵する乱数発生部（図示せず）の乱数に基づいて、共通鍵を生成し、生成された共通鍵をドライブ１１１の公開鍵で暗号化し、ＡＶボード１１２の秘密鍵により暗号化された共通鍵への署名を生成する。また、相互認証部１３１は、内蔵するメモリから、認証局から予め取得され、記憶されているＡＶボード電子証明書を読み出し、暗号化された共通鍵、ＡＶボード１１２による共通鍵への署名、およびＡＶボード電子証明書を、バス１１３を介して、ドライブ１１１に送信する。

ドライブ１１１の相互認証部１２１は、これらを受信し、暗号化された共通鍵をドライブ１１１の秘密鍵で復号して共通鍵（第１の共通鍵）を取得するとともに、ＡＶボード電子証明書を、認証局から予め取得された認証局公開鍵で復号し、ＡＶボード１１２が正当なＡＶボードであることを確認する。また、相互認証部

１２１は、復号されたＡＶボード電子証明書から取得されたＡＶボード１１２の公開鍵により、共通鍵への署名を復号して共通鍵（第２の共通鍵）を取得する。ドライブ１１１の相互認証部１２１は、第１の共通鍵と第２の共通鍵を比較し、両者が等しいと判断された場合、バス１１３上で、共通鍵が改ざんされていないと判断する。これにより、共通鍵が、ドライブ１１１とＡＶボード１１２との間で共有されたことになる。

以上のようにして、ドライブ１１１の相互認証部１２１は、ＡＶボード１１２の相互認証部１３１との間で相互認証処理を実行し、ＡＶボード１１２を相互認証する。これにより、相互認証部１２１および相互認証部１３１は、お互いに、この共通鍵を用いて、コンテンツを暗号化して送信したり、受信したコンテンツを復号することができる。

一方、ＨＤＤ１１４は、ＡＶボード１１２の相互認証部１３１のような相互認証機能を有していない。したがって、ＨＤＤ１１４は、バス１１３上に流れても問題がない（保護しなくてもよい）フリーコンテンツ（保護する必要がないコンテンツ）の送受信をドライブ１１１と実行することができる。

ＡＶボード１１２のＡＶコンテンツ処理部１３３は、入力部１３４を介して放送信号（暗号化またはスクランブルされているコンテンツに対応する信号）を受信すると、予め記憶されている鍵（放送信号を送信する機器と共有している鍵）で暗号化またはスクランブルされているコンテンツを復号し、コンテンツ保護部１３２に供給する。

また、ＡＶコンテンツ処理部１３３は、入力されたコンテンツが、暗号化またはスクランブルされているか否かに基づいて、入力されたコンテンツが保護すべきコンテンツであるか否かという判断を実行することができる。なお、このコンテンツ（放送信号）に、例えば、コンテンツのコピーを制限するために、「Copy Free(コピー可)」，「Copy Once(一世代のみコピー可)」，「No More Copy(この世代以上のコピー不可)」，「Copy Prohibited(コピー禁止)」というコピー世代管理情報(Copy generation management information)を示す、例えば、

ＣＧＭＳ(Copy Generation Management System)信号のようなＣＣＩ(Copy Control Information)が付加されている場合、このコピー世代管理情報が「Copy Free」のときには、入力されたコンテンツが保護すべきコンテンツではないとし、「Copy Once」，「No More Copy」または「Copy Prohibited」のときには、入力されたコンテンツが保護すべきコンテンツであると判断するようにしてもよい。

コンテンツ保護部１３２は、コンテンツをＡＶコンテンツ処理部１３３より入力し、ＡＶコンテンツ処理部１３３によりそのコンテンツが保護すべきコンテンツであると判断された場合、相互認証部１３１より供給された光ディスク１４１のＲＫＢを作用させたディスク鍵を取得し、取得されたディスク鍵および光ディスク１４１のディスクＩＤに基づいて、ブロック鍵を生成する。コンテンツ保護部１３２は、このブロック鍵を用いて、光ディスク１４１上におけるコンテンツ保護のために、保護すべきコンテンツを暗号化し、相互認証部１３１に供給する。

相互認証部１３１は、コンテンツ保護部１３２により暗号化されたコンテンツを、バス１１３上におけるコンテンツ保護のために、ドライブ１１１との共通鍵で暗号化し、バス１１３を介してドライブ１１１に出力する。

なお、ＡＶコンテンツ処理部１３３によりコンテンツが保護すべきコンテンツではないと判断された場合、コンテンツ保護部１３２および相互認証部１３１は、そのコンテンツを暗号化せず、バス１１３を介してドライブ１１１に出力する。

ドライブ１１１の相互認証部１２１は、バス１１３を介してＡＶボード１１２からコンテンツを入力する。また、相互認証部１２１は、入力されたコンテンツが暗号化されている場合、ドライブ１１１との共通鍵で復号し、復号したコンテンツを記録再生処理部１２３に供給する。

入出力制御部１２２は、相互認証部１２１に入力されたコンテンツが、ＡＶボード１１２の相互認証部１３１により、ＡＶボード１１２との共通鍵で暗号化されているか否か（すなわち、ＡＶコンテンツ処理部１３３により保護すべきコンテンツであると判断されたか否か）に基づいて、そのコンテンツがバス１１３上

で保護されるべきコンテンツであるか否かを判断する。そして、入出力制御部１２２は、入力されたコンテンツがバス１１３上で保護されるべきコンテンツであるか否か、かつ、相互認証部１２１によりＡＶボード１１２との間で相互認証がされたか否かに基づいて、記録再生処理部１２３によるコンテンツの記録制御を行う。

また、入出力制御部１２２は、入力されたコンテンツが保護されるべきコンテンツであるか否か、かつ、相互認証部１２１によりＡＶボード１１２との間で相互認証がされたか否かに基づいて、記録再生処理部１２３を制御し、光ディスク１４１に記録されているディスクＩＤおよびＲＫＢ(Renewal Key Block)などの光ディスク１４１のディスク情報を再生させる。

記録再生処理部１２３は、光ディスク１４１にコンテンツを記録する場合、入出力制御部１２２の指示に基づいて、記録するコンテンツが、バス１１３上で保護すべきコンテンツまたはバス１１３上で保護不要のコンテンツであるかを示す保護情報を生成し、その保護情報をコンテンツとともに光ディスク１４１に記録する。

図５は、光ディスク１４１に記録されるデータフォーマットの構成例を示している。

このデータフォーマットにおいては、１フレーム当り２Ｋ（２０４８）バイトで３２フレームのユーザデータ２０１と、１フレーム当り１８バイトで３２フレームのユーザコントロールデータ２０２により、３２セクタが構成されている。

ユーザデータ２０１は、コンテンツのデータなどにより構成される。このユーザデータ２０１は、各フレームに、４つ（４バイト）のＥＤＣ（エラー検出コード）が付加され、図６に示されるようなデータフレーム２０３が構成される。

図６の例においては、１つのデータフレームは、２０５２バイトで構成される。すなわち、１つのデータフレームは、Ｕｄ０乃至Ｕｄ２０４７の番号が振られた２０４８個のユーザデータバイト、およびｅｄ２０４８乃至ｅｄ２０５１の番号が振られた４つのＥＤＣにより構成されている。

このデータフレーム２０３が３２フレーム分集められ、１６×９バイトに配列された物理アドレス２０４に基づいて、図７に示されるようなスクランブルデータフレーム２０５として構成される。

図７の例の場合、１番目の（図中、左端の列の）フレームは、ｄ（０，０），ｄ（１，０），…，ｄ（２０５１，０）の番号が振られた２０５２バイトにより構成され、２番目（図中、左端から２番目の列の）のフレームは、ｄ（０，１），ｄ（１，１），…，ｄ（２０５１，１）の番号が振られた２０５２バイトにより構成される。同様に、Ｆ－１番目のフレームは、ｄ（０，Ｆ），ｄ（１，Ｆ），…，ｄ（２０５１，Ｆ）の番号が振られた２０５２バイトにより構成され、３２番目の（図中、右端の列の）フレームは、ｄ（０，３１），ｄ（１，３１），…，ｄ（２０５１，３１）の番号が振られた２０５２バイトにより構成される。

以上のようなスクランブルデータフレーム２０５から、２１６行３０４列のデータブロック２０６が形成される。データブロック２０６に、３２行のパリティを付加することにより、ＬＤＣ（長距離コード：誤り訂正）ブロック２０７が形成される。ＬＤＣブロック２０７から、１５２列４９６行のＬＤＣクラスタ２０８が形成される。ＬＤＣクラスタ２０８は、それぞれが３８列の４つのＬＤＣ列２０９－１乃至２０９－４に分割され、後述するＢＩＳ列２１３－１乃至２１３－３とによりＥＣＣクラスタ２２１を構成する。

一方、この記録再生装置１０１により付加されるアドレスおよび制御データを説明する。ユーザコントロールデータ（論理アドレスおよび制御データ）２０２は、図８に示されるように、３２×１８バイトに配列される。

図８の例の場合、１番目の（図中、左端の列の）フレームは、ＵＣ（０，０），ＵＣ（１，０），…，ＵＣ（１７，０）の番号が振られた１８バイトにより構成され、２番目の（図中、左端から２番目の列の）フレームは、ＵＣ（０，１），ＵＣ（１，１），…，ＵＣ（１７，１）の番号が振られた１８バイトにより構成される。同様に、Ｓ－１番目のフレームは、ＵＣ（０，Ｓ），ＵＣ（１，Ｓ），…，ＵＣ（１７，Ｓ）の番号が振られた１８バイトにより構成され、３２番目の

（図中、右端の列の）フレームは、ＵＣ（０，３１），ＵＣ（１，３１），…，ＵＣ（１７，３１）の番号が振られた２０５２バイトにより構成される。

上述したように、このデータフォーマットにおいては、各フレーム単位で、２Ｋ（２０４８）バイトのユーザデータ２０１につき、１８バイトのユーザコントロールデータ２０２が対応している。そこで、このユーザデータ２０１（２Ｋバイト）に記録されるデータ（コンテンツ）に対して、バス１１３上で保護すべきコンテンツであるか否かを示す保護情報が生成され、そのユーザデータ２０１に対応するユーザコントロールデータ２０２（１８バイト）の先頭バイトＵＣ（０，Ｓ）の最下位ビットに格納される。

例えば、記録するコンテンツがバス１１３上で保護すべきコンテンツである場合、保護情報として、ユーザコントロールデータ２０２（１８バイト）の先頭バイトＵＣ（０，Ｓ）の最下位ビットに、「０」が生成され、記録される。また、記録するコンテンツがバス１１３上で保護する必要がないコンテンツである場合、保護情報として、ユーザコントロールデータ２０２（１８バイト）の先頭バイトＵＣ（０，Ｓ）の最下位ビットに、「１」が生成され、記録される。なお、既存のデータフォーマットにおいては、ユーザコントロールデータ２０２（１８バイト）の先頭バイトＵＣ（０，Ｓ）の最下位ビットには、もともと「０」が格納されている（未使用とされている）。したがって、既存のデータフォーマットにより記録した保護すべきコンテンツに対しても、バス１１３上で保護すべき情報が格納されていることになるので、既存のものとの互換性を保持することができる。

保護を要するコンテンツの保護情報を「１」とし、保護不要のコンテンツの保護情報を「０」とすることも可能である。しかしながら、そのようにすると、既存のコンテンツはすべてバス１１３上で保護不要のコンテンツとなってしまい、実質的に保護することができなくなってしまう。そこで、保護を要するコンテンツの保護情報を「０」とし、保護不要のコンテンツの保護情報を「１」とするのが好ましい。

また、物理アドレス２０４は、１６×９バイトに配列される。この物理アドレ

ス２０４は、ディスク１４１上の物理的距離に関係する。

３２×１８バイトのユーザコントロールデータ２０２から、物理アドレス２０４に基づいて、２４列×３０行のアクセスブロック２１０が形成される。アクセスブロック２１０は、３２行のパリティが付加され、ＢＩＳ（バースト指示サブコード）ブロック２１１が形成される。ＢＩＳブロック２１１は、３列×４９６行のＢＩＳクラスタ２１２に配列される。

ＢＩＳクラスタ２１２は、ＬＤＣ列２０９－１乃至２０９－４の間に、それぞれが１列の３つのＢＩＳ列２１３－１乃至２１３－３に充填され、１５５列×４９６行のＥＣＣクラスタ２２１が形成される。このＥＣＣクラスタ２２１から、４５チャンネルビットのデータ(data)および１チャンネルビットのコントロールデータ(dc contr.)の４２個の組み合わせにより物理クラスタ２２２が形成され、光ディスク１４１に記録される。

この物理クラスタ２２２は、１９３２チャンネルビット（１２８８データビット）の４９６の記録フレームにグループ化されている。なお、物理クラスタ２２２の最初のデータ(data)のうち、２０チャンネルビットは、同期ビット群(Frame Sync)とされる。

以上のようにして、記録再生処理部１２３により、記録するコンテンツがバス１１３上で保護すべきコンテンツである場合、保護情報として、「０」が生成（格納）され、記録するコンテンツがバス１１３上で保護不要のコンテンツである場合、保護情報として、「１」が生成（格納）され、生成された保護情報がユーザコントロールデータ２０２に記録される。

このデータフォーマットの光ディスク１４１に記録されたコンテンツを再生する場合の誤り訂正動作としては、一般的には、ＢＩＳの誤り訂正動作を行い、ＢＩＳの誤り訂正動作の結果をＬＤＣの誤り訂正動作を行う際の消失情報として用いる。したがって、ＬＤＣの誤り訂正動作が終わって、ユーザデータを出力できるようになる前に、ＢＩＳの誤り訂正動作は終了しているため、ＢＩＳに含まれるユーザコントロールデータは、すでに得られている。したがって、ユーザコン

トロールデータを用いて、ユーザデータの出力制御は可能である。

以上のように、光ディスク１４１に記録された保護情報は、記録再生処理部１２３により、光ディスク１４１に記録されたコンテンツを再生する場合、コンテンツよりも先に再生されるので、この再生された保護情報に基づいて、入出力制御部１２２は、バス１１３へのコンテンツの出力の制御を行う。

例えば、入出力制御部１２２は、相互認証部１２１によりＡＶボード１１２との間で相互認証がされたか否か、および、再生されたコンテンツがバス１１３上で保護されるべきコンテンツであるか（保護情報が「０」であるか）否かに基づいて、相互認証部１２１によるコンテンツのバス１１３への出力制御を行う。相互認証部１２１は、この入出力制御部１２２の制御に基づいて、再生されたコンテンツを、ドライブ１１１との共通鍵で暗号化し、バス１１３を介してＡＶボード１１２に出力する。

このドライブ１１１の相互認証部１２１により暗号化されたコンテンツが入力されると、ＡＶボード１１２の相互認証部１３１は、そのコンテンツを復号し、コンテンツ保護部１３２に供給する。

コンテンツ保護部１３２は、相互認証部１３１によりＡＶボード１１２との共通鍵を用いて復号されたコンテンツを、さらに、光ディスク１４１のディスクＩＤおよびディスク鍵を作用させたブロック鍵により復号し、ＡＶコンテンツ処理部１３３に供給する。ＡＶコンテンツ処理部１３３は、復号されたコンテンツを、例えば、MPEG（Moving Picture Experts Group）方式でデコードし、再生する。出力部１３５は、再生されたコンテンツを出力する。

以上のように、ＡＶボード１１２は、ドライブ１１１と相互認証されているので、著作権などにより保護されるべきコンテンツ（保護すべきコンテンツ）または保護不要のコンテンツをお互いに送受信することができる。

一方、例えば、ＨＤＤ１１４により保護されるべきコンテンツがドライブ１１１に送信されてきたとしても、ＨＤＤ１１４は、ドライブ１１１により相互認証されないので、そのコンテンツは、保護不要のコンテンツであればドライブ１１

１で処理される。すなわち、この記録再生装置１０１において、コピーフリーのコンテンツのみを扱う相互認証しないデータの記録は許可される。

以上のようにして、この記録再生装置１０１においては、著作権などによりコンテンツの保護が必要か否かによって、コンテンツの暗号化またはコンテンツの汎用バスへの出力が柔軟に制御される。

図９は、コンテンツ保護部１３２の構成例を示している。なお、図９においては、説明の便宜上、コンテンツ保護部１３２と光ディスク１４１しか記載されていないが、実際には、コンテンツ保護部１３２と光ディスク１４１との間では、図４に示されるように、相互認証部１３１、バス１１３、相互認証部１２１および記録再生処理部１２３が、それぞれの処理を実行している。

図９の例においては、コンテンツ保護部１３２は、ＲＫＢ処理部２５２、鍵生成部２５３および暗号化部２５４により構成される。

ＲＫＢ処理部２５２は、ＡＶコンテンツ処理部１３３からの入力されたコンテンツが保護されるべきコンテンツであるか否かの情報に基づいて、光ディスク１４１から供給されたＲＫＢ、コンテンツ保護部１３２に予め記憶されているデバイスＩＤおよびデバイス鍵を作用させて、ディスク鍵を取得する（このディスク鍵の取得処理については、特開２００２－８４２７１号公報に開示されており、さらに、図１０乃至図１２を参照して詳しく後述する）。

鍵生成部２５３は、ＲＫＢ処理部２５２により取得されたディスク鍵、光ディスク１４１から供給されたディスクＩＤ、および、コンテンツ保護部１３２に記憶されている記録情報（例えば、ブロックシード、タイトルキーまたは記録モードなどの記録時に使用する情報）を作用させて、ブロック鍵を生成する。

暗号化部２５４は、光ディスク１４１より供給されるコンテンツが暗号化されている場合、鍵生成部２５３により生成されたブロック鍵を用いて、暗号化コンテンツを復号し、ＡＶコンテンツ処理部１３３に出力する。暗号化部２５４は、光ディスク１４１より供給されるコンテンツが暗号化されていない場合、そのコンテンツをそのまま、ＡＶコンテンツ処理部１３３に出力する。

また、暗号化部２５４は、ＡＶコンテンツ処理部１３３からの入力されたコンテンツが保護されるべきコンテンツであるか否かの情報に基づいて、ＡＶコンテンツ処理部１３３より供給されるコンテンツが保護すべきコンテンツである場合、光ディスク１４１上でのコンテンツ保護のために、鍵生成部２５３により生成されたブロック鍵を用いて、コンテンツを暗号化し、光ディスク１４１に供給する。暗号化部２５４は、ＡＶコンテンツ処理部１３３より供給されるコンテンツが保護不要のコンテンツである場合、コンテンツをそのまま（暗号化せずに）、光ディスク１４１に供給する。

次に、ディスク鍵の取得処理に使用されるＲＫＢについて詳しく説明する。図１０は、本発明の記録再生装置１０１の鍵の配布構成を示す図である。図１０の最下段に示すナンバー０乃至１５が個々の記録再生装置（デバイス）に対応する。すなわち、図１０に示される木（ツリー）構造の各葉（リーフ：leaf）がそれぞれ記録再生装置に相当する。

各デバイス０乃至１５は、製造時（出荷時）に、予め設定されている初期ツリーにおける、自分のリーフからルート（最上段）に至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーを自身で格納する。図１０の最下段に示すＫ０００００乃至Ｋ１１１１が、各デバイス０乃至１５にそれぞれ割り当てられたリーフキーであり、最上段のＫＲから、最下段から２番目の節（ノード）に記載されたキーＫＲ乃至Ｋ１１１がノードキーである。

図１０の例においては、例えば、デバイス０は、リーフキーＫ００００と、ノードキーＫ０００，Ｋ００，Ｋ０，ＫＲを所有する。デバイス５は、Ｋ０１０１，Ｋ０１０，Ｋ０１，Ｋ０，ＫＲを所有する。デバイス１５は、Ｋ１１１１，Ｋ１１１，Ｋ１１，Ｋ１，ＫＲを所有する。なお、図１０のツリーには、デバイスが１６個のみ記載され、ツリー構造も４段構成の均衡のとれた左右対称構成として示されているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を有するようにしてもよい。

また、図１０のツリー構造に含まれる各記録再生装置には、様々な記録媒体、

例えば、ＤＶＤ、ＣＤ、ＭＤ（商標）、メモリスティック（登録商標）などを使用する様々なタイプの記録再生装置が含まれている。さらに、様々なアプリケーションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に、図１０に示されるようなキー配布構成が適用される。

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば、図１０の点線で囲まれた部分、すなわち、デバイス０，１，２，３は、同一の記録媒体を用いる１つのグループとして設定される。このツリー構造においては、１つのグループに含まれる４つのデバイス０，１，２，３はノードキーとして共通のキーＫ００，Ｋ０，ＫＲを保有する。このノードキー共有構成を利用することにより、例えば共通のマスター鍵をデバイス０，１，２，３のみに提供することが可能となる。

例えば、共通に保有するノードキーＫ００自体をマスター鍵として設定すれば、新たな鍵送付を実行することなく、デバイス０，１，２，３のみに共通のマスター鍵の設定が可能である。また、新たなマスター鍵Kmasterをノードキー００で暗号化した値Ｅｎｃ（Ｋ００，Kmaster）を、ネットワークを介してあるいは記録媒体に格納してデバイス０，１，２，３に配布すれば、デバイス０，１，２，３のみが、それぞれのデバイスにおいて保有する共有ノードキーＫ００を用いて暗号Ｅｎｃ（Ｋ００，Kmaster）を解いてマスター鍵Kmasterを得ることが可能となる。なお、Ｅｎｃ（Ｋａ，Ｋｂ）はＫｂをＫａによって暗号化したデータであることを示す。

また、ある時点ｔにおいて、デバイス３の所有する鍵Ｋ００１１，Ｋ００１，Ｋ００，Ｋ０，ＫＲが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。そのためには、ノードキーＫ００１，Ｋ００，Ｋ０，ＫＲをそれぞれ新たな鍵：Ｋ（ｔ）００１，Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒに更新し、デバイス０，１，

２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Generation）：ｔの更新キーであることを示す。

更新キーの配布処理について説明する。キーの更新は、例えば、図１１Ａに示すＲＫＢ（Renewal Key Block）と呼ばれるブロックデータによって構成されるテーブルを、たとえばネットワーク、あるいは記録媒体に格納してデバイス０，１，２に供給することによって実行される。

図１１Ａに示すＲＫＢには、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図１１Ａは、図１０に示されるツリー構造中のデバイス０，１，２において、世代ｔの更新ノードキーを配布することを目的として形成されたブロックデータの例を示す。上述したように、デバイス０，デバイス１は、更新ノードキーとしてＫ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒが必要であり、デバイス２は、更新ノードキーとしてＫ（ｔ）００１，Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒが必要である。

図１１ＡのＲＫＢに示されるように、ＲＫＢには複数の暗号化キーが含まれる。最下段の暗号化キーは、Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）００１）である。これはデバイス２の持つリーフキーＫ００１０によって暗号化された更新ノードキーＫ（ｔ）００１であり、デバイス２は、自身の持つリーフキーによってこの暗号化キーを復号し、Ｋ（ｔ）００１を得ることができる。また、復号により得たＫ（ｔ）００１を用いて、図１１Ａの下から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００１，Ｋ（ｔ）００）が復号可能となり、更新ノードキーＫ（ｔ）００を得ることができる。以下、順次、図１１Ａの上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図１１Ａの上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号し、Ｋ（ｔ）Ｒが得られる。

一方、ノードキーＫ０００は更新する対象に含まれておらず、デバイス０，１が、更新ノードキーとして必要とするのは、Ｋ（ｔ）００，Ｋ（ｔ）０，Ｋ（ｔ）Ｒである。デバイス０，１は、図１１Ａの上から３段目の暗号化キーＥｎ

ｃ（Ｋ０００，Ｋ（ｔ）００）を復号し、Ｋ（ｔ）００を取得し、以下、図１１Ａの上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０を得、図１１Ａの上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号し、Ｋ（ｔ）Ｒを得る。このようにして、デバイス０，１，２は更新した鍵Ｋ（ｔ）Ｒを得ることができる。なお、図１１Ａのインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

図１０に示すツリー構造の上位２段のノードキーＫ０，ＫＲの更新が不要であり、ノードキーＫ００のみの更新処理が必要である場合には、図１１ＢのＲＫＢを用いることで、更新ノードキーＫ（ｔ）００をデバイス０，１，２に配布することができる。

図１１Ｂに示すＲＫＢは、例えば、特定のグループにおいて共有する新たなマスター鍵を配布する場合に利用可能である。具体例として、図１０に、点線で示すグループ内のデバイス０，１，２，３がある記録媒体を用いており、新たな共通のマスター鍵Ｋ（ｔ）master が必要であるとする。このとき、デバイス０，１，２，３の共通のノードキーＫ００を更新したＫ（ｔ）００を用いて新たな共通の更新マスター鍵Ｋ（ｔ）master を暗号化したデータＥｎｃ（Ｋ（ｔ），Ｋ（ｔ）master）を、図１１Ｂに示すＲＫＢとともに配布する。この配布により、デバイス４など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

すなわち、デバイス０，１，２，３はＲＫＢを処理して得たＫ（ｔ）００を用いて上記暗号文を復号すれば、ｔ時点でのマスター鍵Ｋ（ｔ）master を得ることが可能になる。

以上においては、ＲＫＢを用いて、各記録再生装置に対してマスター鍵を伝送し、これを用いて記録再生装置がデータの記録、再生を行う例を説明したが、本発明においては、上述したマスター鍵として、記録媒体のみに限定されたものであるディスク鍵が使用される。このディスク鍵は、図１２に示されるように、記

録媒体のＲＫＢ(Renewal Key Block)を用いて生成される。なお、ディスク鍵Ｋ（ｔ）mediaは、マスター鍵をその記録媒体のみに限定したものであり、基本的な構成は、上述したマスター鍵と同様であるため、その説明を省略する。

図１２の例の場合、デバイス０が、記録媒体に格納されている世代：ｔ時点のＲＫＢと、自分があらかじめ格納しているリーフキーＫ００００と、ノードキーＫ０００，Ｋ００を用いて更新ノードキーＫ（ｔ）００を生成し、それを用いて更新ディスク鍵Ｋ（ｔ）mediaを得る様子を示している。ここで得たＫ（ｔ）mediaは、その記録媒体のデータの記録、再生時に使用される。

なお、図１２におけるプレ記録世代番号（Generation #n）は、ディスク鍵においてはマスター鍵のように世代の新旧という概念はないので必須ではなくオプションとして設定される。

以上のようにして、光ディスク１４１からのＲＫＢ、コンテンツ保護部１３２のデバイスＩＤ（例えば、図１０のデバイス０）、デバイス鍵（例えば、図１０のデバイス０におけるリーフキーＫ００００）およびノードキー（図１０のデバイス０におけるＫ０００，Ｋ００，…）などに基づいて、ディスク鍵が取得される。このディスク鍵の取得処理は、例えば、コンテンツの記録もしくは再生のために、光ディスク１４１が記録再生装置１０１のドライブ１１１に装着された際に実行されるようにしてもよいし、または、光ディスク１４１が装着されており、コンテンツの記録もしくは再生を指示した際に実行されるようにしてもよい。

次に、図１３のフローチャートを参照して、記録再生装置１０１のＡＶボード１１２の相互認証処理について説明する。

ドライブ１１１とＡＶボード１１２が接続され、それぞれの電源がオンされたとき、ステップＳ１１において、ＡＶボード１１２の相互認証部１３１は、内蔵する乱数発生部の乱数に基づいて、共通鍵を生成する。ステップＳ１２において、相互認証部１３１は、生成された共通鍵をドライブ１１１の公開鍵で暗号化する。ステップＳ１３において、相互認証部１３１は、ＡＶボード１１２の秘密鍵により暗号化された共通鍵への署名を生成する。ステップＳ１４において、相互認証

部１３１は、内蔵するメモリより、図示せぬ認証局から予め取得され、記憶されているＡＶボード電子証明書を読み出す。ステップＳ１５において、相互認証部１３１は、暗号化された共通鍵、ＡＶボード１１２による共通鍵への署名、およびＡＶボード電子証明書を、バス１１３を介して、ドライブ１１１に送信する。

このようにして、ＡＶボード１１２から、暗号化された共通鍵、ＡＶボード１１２による共通鍵への署名、およびＡＶボード電子証明書がドライブ１１１に送信される。このＡＶボード１１２の相互認証処理に対応するドライブ１１１の相互認証処理を、図１４のフローチャートを参照して説明する。

ステップＳ３１において、ドライブ１１１の相互認証部１２１は、受信したＡＶボード電子証明書を、予め取得してあるか、その都度取得する認証局公開鍵に基づいて復号する。ステップＳ３２において、相互認証部１２１は、ステップＳ３１において復号されたＡＶボード電子証明書に基づいて、ＡＶボード１１２が正当なＡＶボードであるか否かを判断する。ＡＶボード電子証明書が復号できなかったり、改ざんされている場合には、ステップＳ３２において、ＡＶボード１１２が正当なＡＶボードではないと判断され、処理は終了する。

ステップＳ３２において、ＡＶボード１１２が正当なＡＶボードであると判断された場合、ＡＶボード電子証明書を復号することによりＡＶボード１１２の公開鍵が得られる。相互認証部１２１は、ステップＳ３３において、暗号化されている共通鍵を、ドライブ１１１の秘密鍵を用いて復号する。ステップＳ３４において、相互認証部１２１は、ＡＶボード１１２による共通鍵への署名を、ＡＶボード１１２の公開鍵を用いて復号する。

ステップＳ３５において、相互認証部１２１は、ステップＳ３３において復号された共通鍵と、署名に平文で添付されている共通鍵を比較し、両者が一致するか否かを判断する。これにより、その共通鍵が正当な共通鍵であるか否かが判定される。ステップＳ３５において、共通鍵と、署名の共通鍵が一致すると判断された場合、相互認証部１２１は、ＡＶボード１１２から正当な共通鍵が送信されてきたと判定し、ステップＳ３６において、共通鍵を記憶する。一方、ステップ

Ｓ３５において、共通鍵と、署名の共通鍵が一致しないと判断された場合、相互認証部１２１は、ＡＶボード１１２とドライブ１１１との間において、共通鍵が改ざんされているとし、処理を終了する。

以上のようにして、ドライブ１１１とＡＶボード１１２との間で、相互認証が行われ、共通鍵が共有されている状態において、これ以降の処理が実行される。

なお、説明は省略するが、さらに、ドライブ１１１の相互認証部１２１が、ＡＶボード１１２から取得した共通鍵をドライブ１１１の公開鍵で暗号化したもの、それに対するドライブ１１１による署名、およびドライブ電子証明書を、ＡＶボード１１２に送信し、ＡＶボード１１２に認証させるようにしてもよい。

次に、図１５のフローチャートを参照して、記録再生装置１０１のＡＶボード１１２の記録要求処理について説明する。

ステップＳ１０１において、ＡＶコンテンツ処理部１３３は、コンテンツが入力されるまで待機している。ＡＶコンテンツ処理部１３３は、アンテナなどにより構成される入力部１３４を介して放送信号（コンテンツに対応する信号）を受信すると、ステップＳ１０１において、コンテンツが入力されたと判断し、ステップＳ１０２において、入力されたコンテンツが暗号化またはスクランブルされているか否かに基づいて、入力されたコンテンツが保護すべきコンテンツであるか否かを判断する。

ステップＳ１０２において、ＡＶコンテンツ処理部１３３は、そのコンテンツが保護すべきコンテンツであると判断した場合、暗号化またはスクランブルされているコンテンツを、予め記憶されている鍵（放送信号を送信する機器と共有している鍵）で復号し、ステップＳ１０３において、ＡＶコンテンツ処理部１３３は、コンテンツ保護部１３２にブロック鍵生成処理を実行させる。このブロック鍵生成処理を、図１６のフローチャートを参照して説明する。なお、図１６のＡＶボード１１２におけるブロック鍵生成処理に対応するドライブ１１１のドライブ情報取得処理も、図１７のフローチャートを参照して、合わせて説明する。

ステップＳ１２１において、ＲＫＢ処理部２５２は、光ディスク１４１のディ

スク情報（例えば、ディスクＩＤおよびＲＫＢ）の読み出しの要求を、ドライブ１１１に出力する。具体的には、ＲＫＢ処理部２５２は、光ディスク１４１のディスクＩＤおよびＲＫＢの読み出しの要求を、相互認証部１３１に出力する。相互認証部１３１は、ディスクＩＤおよびＲＫＢの読み出しの要求を、バス１１３を介して、ドライブ１１１の相互認証部１２１に出力する。

ステップＳ１４１において、ドライブ１１１の相互認証部１２１は、バス１１３を介して、ＡＶボード１１２からの光ディスク１４１のディスクＩＤおよびＲＫＢの読み出しの要求を受信する。

ステップＳ１４２において、入出力制御部１２２は、相互認証部１２１からの情報に基づいて、このディスクＩＤおよびＲＫＢの読み出しの要求をするＡＶボード１１２が、ドライブ１１１において相互認証されているか否かを判断する。ステップＳ１４２において、ＡＶボード１１２が、ドライブ１１１において相互認証されていないと判断された場合、ドライブ１１１のディスク情報再生処理は終了する。これにより、不正な装置からの要求は拒絶される。

上述したように、ＡＶボード１１２は、ドライブ１１１において相互認証されているので、ステップＳ１４２において、ＡＶボード１１２が、ドライブ１１１において相互認証されていると判断される。この場合、ステップＳ１４３において、記録再生処理部１２３は、光ディスク１４１に記録されているディスクＩＤおよびＲＫＢを再生し、相互認証部１２１に供給する。

ステップＳ１４４において、相互認証部１２１は、記録再生処理部１２３により供給されたディスクＩＤおよびＲＫＢを、ＡＶボード１１２との共通鍵を用いて暗号化し、バス１１３を介して、ＡＶボード１１２に出力する。

ステップＳ１２２において、ＡＶボード１１２の相互認証部１３１は、バス１１３を介して、暗号化されているディスクＩＤおよびＲＫＢを受信し、ドライブ１１１との共通鍵を用いて復号し、ＲＫＢ処理部２５１に供給する。

ステップＳ１２３において、ＲＫＢ処理部２５１は、供給されたＲＫＢと内蔵するメモリに予め記憶されているデバイスＩＤおよびデバイスキーを作用させて、

ディスク鍵を取得する。具体的には、ＲＫＢ処理部２５１は、供給されたＲＫＢと、自身がメモリに記憶しているデバイスＩＤ（例えば、図１０のデバイス０）、デバイスキー（例えば、図１０のデバイス０におけるリーフキーＫ０００００）、およびノードキー（例えば、図１０のデバイス０におけるＫ０００，Ｋ００，Ｋ０，ＫＲ）を用いて、プレ記録世代情報Generation #n（例えば、図１２におけるｔ）時点でのノード００の鍵Ｋ（ｔ）００を計算する。そして、ＲＫＢ処理部２５１は、供給されたＲＫＢの中から、ディスク鍵Ｋ（ｔ）mediaを、鍵Ｋ（ｔ）００で暗号化した暗号文Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）media）を取得し、これを復号して、ディスク鍵Ｋ（ｔ）mediaを取得する。

ステップＳ１２４において、鍵生成部２５３は、相互認証部１３１より供給されたディスクＩＤ、ステップＳ１２３において取得されたディスク鍵、および、コンテンツ保護部１３２の記録情報などを作用させて、ブロック鍵を生成し、暗号化部２５４に内蔵されるメモリなどに記憶する。

以上のようにしてブロック鍵が生成されるので、図１５のステップＳ１０４において、暗号化部２５４は、ＡＶコンテンツ処理部１３３より供給されたコンテンツを、ステップＳ１２４において生成されたブロック鍵で暗号化し、相互認証部１３１に出力する。

相互認証部１３１は、ステップＳ１０５において、ステップＳ１０４においてブロック鍵で暗号化されたコンテンツを、さらに、ドライブ１１１との共通鍵を用いて、暗号化し、ステップＳ１０６において、バス１１３を介してドライブ１１１に出力する。

一方、ステップＳ１０２において、ＡＶコンテンツ処理部１３３より入力されたコンテンツが保護不要のコンテンツであると判断された場合、そのコンテンツは、暗号化部２５４において暗号化する（光ディスク１４１上で保護する）必要がなく、相互認証部１３１においても暗号化する（バス１１３上で保護する）必要がないため、ステップＳ１０３乃至Ｓ１０５の処理は、スキップされる。すなわち、暗号化部２５４は、そのコンテンツを暗号化させずに（生データのまま

で）、相互認証部１３１に出力する。ステップＳ１０６において、相互認証部１３１は、暗号化されていないコンテンツを、バス１１３を介して、ドライブ１１１に出力する。

以上のようにして、ＡＶボード１１２からは、保護すべきコンテンツは、ＲＫＢおよびディスクＩＤを作用させたブロック鍵で暗号化される。さらに、保護すべきコンテンツは、ドライブ１１１との共通鍵で一時的に暗号化され、バス１１３に出力される。また、保護不要のコンテンツは、生データのまま、バス１１３に出力される。これに対応して実行されるドライブ１１１の記録処理を、図１８のフローチャートを参照して説明する。

ステップＳ１６１において、ドライブ１１１の相互認証部１２１は、バス１１３を介して、ＡＶボード１１２よりコンテンツを受信する。

ステップＳ１６２において、入出力制御部１２２は、相互認証部１２１からの情報に基づいて、コンテンツを入力してきた装置が、ドライブ１１１において相互認証されているか否かを判断する。ステップＳ１６２において、ＡＶボード１１２が、ドライブ１１１において相互認証されていると判断された場合、ステップＳ１６３において、入出力制御部１２２は、相互認証部１２１に入力されたコンテンツが共通鍵で暗号化されているか否かに基づいて、入力されたコンテンツの記録コマンドが、バス１１３上で保護すべきコンテンツの記録コマンドであるかを判断する。

ステップＳ１６３において、このコンテンツの記録コマンドが、バス１１３上で保護すべきコンテンツの記録コマンドであると判断された場合、ステップＳ１６４において、入出力制御部１２２は、相互認証部１２１を制御し、受信したコンテンツを、ＡＶボード１１２との共通鍵で復号させる。したがって、いま、このコンテンツは、ディスクＩＤおよびＲＫＢを作用させたブロック鍵にのみ暗号化された状態となる。

入出力制御部１２２は、記録再生処理部１２３を制御し、ステップＳ１６５において、このコンテンツに対応するユーザコントロールデータのＵＣ（０，Ｓ）

に、バス１１３上で保護すべきコンテンツであるという保護情報「０」を生成、格納させ、ステップＳ１６８において、ブロック鍵で暗号化された状態のコンテンツとともに、光ディスク１４１に記録させる。

一方、例えば、相互認証部を有しないＨＤＤ１１４に記憶されているコンテンツが入力される。この場合、ステップＳ１６１において、ＨＤＤ１１４からコンテンツが、バス１１３を介して、相互認証部１２１に受信される。ＨＤＤ１１４は、相互認証部を有しないので、ステップＳ１６２において、コンテンツを入力してきた装置が、ドライブ１１１において相互認証されていないと判断され、処理は、ステップＳ１６６に進む。ステップＳ１６６において、入出力制御部１２２は、相互認証部１２１に入力されたコンテンツが共通鍵で暗号化されているか否かに基づいて、入力されたコンテンツの記録コマンドが、バス１１３上で保護すべきコンテンツの記録コマンドであるか否かを判断する。

ステップＳ１６３において、または、ステップＳ１６６において、入力されたコンテンツの記録コマンドが、バス１１３上で保護不要のコンテンツの記録コマンドであると判断された場合、ステップＳ１６７において、入出力制御部１２２は、記録再生処理部１２３を制御し、コンテンツに対応するユーザコントロールデータのＵＣ（０，Ｓ）に、バス１１３上で保護不要のコンテンツであるという保護情報「１」を生成（格納）させ、生成された保護情報を、ステップＳ１６８において、暗号化されていないコンテンツとともに、光ディスク１４１に記録させる。

また、ステップＳ１６６において、入力されたコンテンツの記録コマンドが、バス１１３上で保護すべきコンテンツの記録コマンドであると判断された場合、エラーとなり、ドライブ１１１の記録処理は、強制的に終了される。したがって、ドライブ１１１においては、相互認証されないＨＤＤ１１４からのコンテンツは、バス１１３上で保護すべきコンテンツとしては記録されない。

以上のように、相互認証されているＡＶボード１１２からの保護すべきコンテンツは、バス１１３上で保護すべきコンテンツであるという保護情報「０」とと

もに光ディスク１４１に記録される。この場合、保護すべきコンテンツは、ディスクＩＤおよびＲＫＢを作用させたブロック鍵により暗号化されている。また、相互認証されているＡＶボード１１２からの保護不要のコンテンツ、または、相互認証されていないＨＤＤ１１４からの保護不要のコンテンツは、バス１１３上で保護不要のコンテンツであるという保護情報「１」とともに光ディスク１４１に記憶される。この場合、保護不要のコンテンツは、暗号化されていない。

以上のようにして格納された保護情報は、次に説明するドライブ１１１のコンテンツ再生処理により再生され、利用される。図１９のフローチャートを参照して、ドライブ１１１のコンテンツ再生処理について説明する。

ユーザは、光ディスク１４１に記録されている保護すべきコンテンツを、ＡＶボード１１２の出力部１３５から出力させるために、図示せぬ操作入力部などを介して、ＡＶボード１１２に、コンテンツの再生コマンドを入力する。ＡＶボード１１２の相互認証部１３１は、バス１１３を介して、ドライブ１１１に再生コマンドを送信してくるので、ステップＳ１９１において、相互認証部１２１は、ＡＶボード１１２からの再生コマンドを入力する。

ステップＳ１９２において、入出力制御部１２２は、相互認証部１２１からの情報に基づいて、コンテンツを出力する機器（いまの場合、ＡＶボード１１２）が、ドライブ１１１において相互認証されているか否かを判断する。ステップＳ１９２において、ＡＶボード１１２が相互認証されていると判断された場合、ステップＳ１９３において、入出力制御部１２２は、ＡＶボード１１２からの再生コマンドが、保護すべきコンテンツの再生コマンドであるか否かを判断する。

ステップＳ１９３において、ＡＶボード１１２からの再生コマンドが、保護すべきコンテンツの再生コマンドであると判断された場合、ステップＳ１９４において、記録再生処理部１２３は、光ディスク１４１から指示されたコンテンツを再生する。

図５を参照して上述したように、光ディスク１４１に記録された保護情報（ユーザコントロールデータ）は、コンテンツを再生する場合、そのコンテンツより

も先に再生されるので、ステップＳ１９５において、入出力制御部１２２は、そのコンテンツに対応するユーザコントロールデータのＵＣ（０，Ｓ）が「０」であるか否かを判断し、コンテンツに対応するＵＣ（０，Ｓ）が「０」であると判断された場合、このコンテンツはバス１１３上で保護すべきコンテンツであることになるので、ステップＳ１９６において、入出力制御部１２２は、相互認証部１２１を制御し、ＡＶボード１１２との共通鍵を用いて、再生されたコンテンツを暗号化させ、バス１１３を介してＡＶボード１１２に出力させる。したがって、バス１１３上における不正なデータの取得（ハッキング）が防止される。

ステップＳ１９５において、コンテンツに対応するＵＣ（０，Ｓ）が「０」ではないと判断された場合（コンテンツに対応するＵＣ（０，Ｓ）が「１」であると判断された場合）、このコンテンツは、バス１１３上で保護不要のコンテンツであるため、ＡＶボード１１２からの保護すべきコンテンツの再生コマンドと矛盾するため、ドライブ１１１の再生処理は終了する。すなわち、ドライブ１１１は、バス１１３上へのデータの出力を行わないように制御される。

一方、例えば、ユーザは、光ディスク１４１に記録されている保護不要のコンテンツを、ＨＤＤ１１４に保存（記録）させるために、図示せぬ操作入力部などを介して、ＨＤＤ１１４に、コンテンツの再生コマンドを入力する。ＨＤＤ１１４は、バス１１３を介して、ドライブ１１１に再生コマンドを送信してくるので、ステップＳ１９１において、相互認証部１２１は、ＨＤＤ１１４からの再生コマンドを入力する。

ステップＳ１９２において、入出力制御部１２２は、相互認証部１２１からの情報に基づいて、コンテンツを出力する機器（いまの場合、ＨＤＤ１１４）が、相互認証されていないと判断する。このとき、ステップＳ１９７において、入出力制御部１２２は、ＨＤＤ１１４からの再生コマンドが、保護すべきコンテンツの再生コマンドであるか否かを判断する。

ステップＳ１９３において、または、ステップＳ１９７において、コンテンツを出力する機器からの再生コマンドが、保護不要のコンテンツの再生コマンドで

あると判断された場合、ステップＳ１９８において、記録再生処理部１２３は、光ディスク１４１から指示されたコンテンツを再生する。ステップＳ１９９において、入出力制御部１２２は、そのコンテンツに対応するユーザコントロールデータのＵＣ（０，Ｓ）が「１」であるか否かを判断する。コンテンツに対応するＵＣ（０，Ｓ）が「１」であると判断された場合、このコンテンツがバス１１３上で保護不要のコンテンツであることになるので、ステップＳ２００において、入出力制御部１２２は、相互認証部１２１を制御し、再生されたコンテンツをそのまま（生データのまま）、バス１１３を介してコンテンツを出力する機器（いまの場合、ＡＶボード１１２またはＨＤＤ１１４）に出力させる。

また、ステップＳ１９７において、ＨＤＤ１１４からのコマンドが、保護すべきコンテンツの再生コマンドであると判断された場合、または、ステップＳ１９９において、コンテンツに対応するＵＣ（０，Ｓ）が「１」ではないと判断された場合（コンテンツに対応するＵＣ（０，Ｓ）が「０」であると判断された場合）、相互認証されていないＨＤＤ１１４へは、保護すべきコンテンツの出力はできないので、エラーとなり、ドライブ１１１の出力処理は、強制的に終了される。すなわち、ドライブ１１１においては、ＨＤＤ１１４から保護すべきコンテンツの再生コマンドは拒否される。また、保護不要のコンテンツの再生コマンドであったとしても、実際にバス１１３上において、保護すべきコンテンツであった場合は、出力されない。

以上のようにして、相互認証されているＡＶボード１１２への再生コマンドに対して、バス１１３上で保護すべきコンテンツは、共通鍵で暗号化され、バス１１３を介して、ＡＶボード１１２に出力され、バス１１３上で保護不要のコンテンツは、そのまま（暗号化させずに）、バス１１３を介して、ＡＶボード１１２に出力される。そして、後述する図２０のステップＳ２０１において、ＡＶボード１１２の相互認証部１３１により受信される。

一方、相互認証されていないＨＤＤ１１４への再生コマンドに対しては、バス１１３上で保護すべきコンテンツは、出力されないが、バス１１３上で保護不要

のコンテンツは、そのまま（暗号化させずに）、バス１１３を介して、ＨＤＤ１１４に出力される。これにより、ＨＤＤ１１４において、保護不要のコンテンツが記憶できるので、ストレージ運用が可能になる。

また、保護されるべきコンテンツは、ディスクＩＤおよびＲＫＢを作用させたブロック鍵、およびコンテンツを送受信する装置間（いまの場合、ドライブ１１１およびＡＶボード１１２）における相互認証されている共通鍵の両方で暗号化されているため、汎用的なバス１１３を介しても、不当なコピーを抑制することができる。

なお、既存の記録再生装置において光ディスクに記録された保護すべきコンテンツに対応するユーザコントロールデータ２０２（１８バイト）の先頭バイトＵＣ（０，Ｓ）の最下位ビットには、もともと「０」が格納されている。したがって、既存のデータフォーマットにより記録した保護すべきコンテンツに対しても、上述した保護すべきコンテンツの再生処理が実行される（相互認証されている機器に対しては、共通鍵で暗号されて出力され、相互認証されていない機器に対しては、出力が禁止される）ので、汎用的なバス１１３を介しても、不当なコピーを抑制することができる。すなわち、既存のものとの互換性が保たれる。

以上のようなドライブ１１１のコンテンツ再生処理に対応するＡＶボード１１２の再生処理を、図２０のフローチャートを参照して説明する。

ドライブ１１１は、ＡＶボード１１２からの保護すべきコンテンツの再生コマンドを受信し、光ディスク１４１よりコンテンツを再生し、バス１１３を介して出力してくるので、ＡＶボード１１２の相互認証部１３１は、ステップＳ２０１において、そのコンテンツを受信し、ステップＳ２０２において、受信したコンテンツが、ドライブ１１１の相互認証部１２１により暗号化されているか（保護すべきコンテンツであるか）否かを判断する。

ステップＳ２０２において、そのコンテンツが、共通鍵を用いて暗号化されており、保護すべきコンテンツであると判断された場合、ステップＳ２０３において、相互認証部１３１は、ドライブ１１１との共通鍵を用いて、受信されたコン

テンツを復号し、コンテンツ保護部１３２に出力する。すなわち、いま、このコンテンツは、ディスクＩＤおよびＲＫＢを作用させたブロック鍵のみにより暗号化されている状態である。

ステップＳ２０４において、コンテンツ保護部１３２は、ブロック鍵の生成処理を実行する。なお、このブロック鍵の生成処理は、図１６を参照して説明したブロック鍵生成処理と同様であるので、その説明は繰り返しになるので、省略するが、ステップＳ２０４において、光ディスク１４１のＲＫＢを作用させたディスク鍵が取得され、取得されたディスク鍵および光ディスク１４１のディスクＩＤが生成されるので、ステップＳ２０５において、暗号化部２５４は、相互認証部１３１からのコンテンツを、ブロック鍵を用いて復号し、ＡＶコンテンツ処理部１３３に供給する。

一方、ステップＳ２０２において、受信したコンテンツが、暗号化されておらず、保護不要のコンテンツであると判断された場合、このコンテンツは復号する必要はない。したがって、相互認証部１３１およびコンテンツ保護部１３２を素通りするため、ステップＳ２０３乃至Ｓ２０５の処理はスキップされる。

ステップＳ２０６において、ＡＶコンテンツ処理部１３３は、コンテンツ保護部１３２から供給されたコンテンツを、例えば、MPEG（Moving Picture Experts Group）方式でデコードし、再生する。ステップＳ２０７において、出力部１３５は、再生されたコンテンツを出力する。

以上のようにして、ドライブ１１１と相互認証されているＡＶボード１１２においては、光ディスク１４１に記録されている保護すべきコンテンツおよび保護不要のコンテンツの両方を出力することができる。

なお、上記説明においては、ＡＶボード１１２は、記録時および再生時に、保護すべきコンテンツであると判断してからブロック鍵を生成するように説明したが、このブロック鍵の生成処理は、光ディスク１４１が装着されるごとにＡＶボード１１２の保護コンテンツ部１３２において実行されるようにしてもよい。

図２１は、本発明の記録再生装置の他の構成例を示している。なお、図２１の

記録再生装置３０１の基本的な構成は、図４の記録再生装置１０１と同様であるが、図２１の記録再生装置３０１においては、図４の記録再生装置１０１におけるドライブ１１１の相互認証部１２１が除かれている。

したがって、図２１の記録再生装置３０１においては、ＡＶボード１１２は、バス１１３上に接続されていても、ドライブ１１１が、相互認証機能を有しないため、ＡＶボード１１２において相互認証されず（共通鍵が共有されず）、ＡＶボード１１２からのコンテンツの再生要求処理は実行されないが、相互認証機能を有しないＨＤＤ１１４との保護不要のコンテンツの送受信処理が実行される。

この記録再生装置３０１のドライブ１１１の記録処理を、図２２のフローチャートを参照して説明する。なお、図２２のステップＳ２１１乃至Ｓ２１４は、図１８のステップＳ１６１およびステップＳ１６６乃至Ｓ１６８と同様の処理であり、その詳細な説明は繰り返しになるので省略する。

ステップＳ２１１において、ＨＤＤ１１４からの保護不要のコンテンツが、バス１１３を介して記録再生処理部１２３に受信される。ステップＳ２１２において、入出力制御部１２２により、記録再生処理部１２３に入力されたコンテンツが共通鍵で暗号化されていないので、いまの記録コマンドが、バス１１３上で保護すべきコンテンツの記録コマンドではないと判断される。ステップＳ２１３において、記録再生処理部１２３により、コンテンツに対応するユーザコントロールデータのＵＣ（０，Ｓ）に、バス１１３上で保護不要のコンテンツであるという保護情報「１」が生成、格納され、ステップＳ２１４において、記録再生処理部１２３により、このＨＤＤ１１４からの保護不要のコンテンツが光ディスク１４１に記録される。

また、ステップＳ２１２において、共通鍵で暗号化されているコンテンツが入力され、いまの記録コマンドが、保護すべきコンテンツの記録コマンドであると判断された場合、エラーとなり、ドライブ１１１の記録処理は、強制的に終了される。

以上のようにして、相互認証機能を有さないＨＤＤ１１４からのバス１１３上

で保護不要の保護情報ともに、コンテンツが光ディスク１４１に記録される。

次に、この記録再生装置３０１のドライブ１１１の再生処理を、図２３のフローチャートを参照して説明する。なお、図２３のステップＳ２２１乃至Ｓ２２５の処理は、図１９のステップＳ１９１およびステップＳ１９７乃至Ｓ２００の処理と同様の処理であり、その詳細な説明は繰り返しになるので省略する。

したがって、例えば、ユーザは、光ディスク１４１に記録されている保護不要のコンテンツを、ＨＤＤ１１４に保存（記録）させるために、入力部を介して、ＨＤＤ１１４へのコンテンツの再生コマンドを入力する。ＨＤＤ１１４は、バス１１３を介して、ドライブ１１１に再生コマンドを送信してくる。ステップＳ２２１において、ＨＤＤ１１４からの再生コマンドが入力される。ステップＳ２２２において、入出力制御部１２２により、ＨＤＤ１１４からの再生コマンドが、保護不要のコンテンツの再生コマンドであると判断された場合、ステップＳ２２３において、記録再生処理部１２３により、指示されたコンテンツが光ディスク１４１から再生される。

ステップＳ２２４において、入出力制御部１２２により、そのコンテンツに対応するユーザコントロールデータのＵＣ（０，Ｓ）が「１」であると判断された場合、バス１１３上で保護不要のコンテンツであるとされる。ステップＳ２２５において、記録再生処理部１２３により再生されたコンテンツがそのまま（生データのまま）、バス１１３を介してＨＤＤ１１４に出力される。

一方、ステップＳ２２２において、ＨＤＤ１１４からのコマンドが、保護すべきコンテンツの再生コマンドであると判断された場合、または、ステップＳ２２４において、コンテンツに対応するＵＣ（０，Ｓ）が「１」ではないと判断された場合、相互認証されていないＨＤＤ１１４へは、バス１１３上において保護すべきコンテンツの出力はできないので、エラーとなり、ドライブ１１１の記録処理は、強制的に終了される。

以上のようにして、ＨＤＤ１１４への再生コマンドに対して、保護情報「１」が再生された場合、再生された、バス１１３上での保護不要のコンテンツは、そ

のまま（暗号化させずに）、バス１１３を介して、ＨＤＤ１４に出力される。したがって、保護不要のコンテンツは、共通鍵により暗号化もされていないので、ＨＤＤ１４に供給され、記憶されるようにできる。これにより、ＨＤＤ１４において、ストレージ運用が可能になる。

図２４は、本発明を適用したさらに他の記録再生装置の構成例を示している。図２４の記録再生装置４０１は、図４の記録再生装置１０１と基本的に同様な構成とされるが、図２４のＡＶボード１１２においては、図４のＡＶボード１１２のコンテンツ保護部１３２が除かれており、代わりに、ドライブ１１１にコンテンツ保護部４１１が配置されている構成になっている。

したがって、図２４のＡＶボード１１２においては、ＡＶコンテンツ処理部１３３から供給されるコンテンツは、相互認証部１３１に出力される。相互認証部１３１より出力されるコンテンツは、ＡＶコンテンツ処理部１３３に供給される。

また、図２４のドライブ１１１においては、相互認証部１２１に入力されたコンテンツは、コンテンツ保護部４１１に供給される。コンテンツ保護部４１１の基本的な構成は、図４のコンテンツ保護部１３２と同様である。したがって、コンテンツ保護部４１１は、相互認証部１２１から供給されたコンテンツを、入出力制御部１２２の制御のもと、光ディスク１４１のディスクＩＤおよびＲＫＢ（ディスク鍵）を作用させたブロック鍵、または、ＲＫＢ（ディスク鍵）のみを作用させたブロック鍵により暗号化し、記録再生処理部１２３に出力する。

記録再生処理部１２３は、光ディスク１４１から再生されたコンテンツを、コンテンツ保護部４１１に供給する。コンテンツ保護部４１１は、入出力制御部１２２の制御のもと、光ディスク１４１のディスクＩＤおよびＲＫＢを作用させたブロック鍵、または、ＲＫＢのみを作用させたブロック鍵により復号し、相互認証部１２１に出力する。

図２５は、図２４のコンテンツ保護部４１１の構成を示している。なお、図２４のコンテンツ保護部４１１は、図９のコンテンツ保護部１３２と基本的に同様の構成を有している。したがって、例えば、入出力制御部１２２により、ＡＶボ

ード１１２からの入力されたコンテンツが保護すべきコンテンツである（入力されたコンテンツの記録コマンドが、保護すべきコンテンツの記録コマンドである）と判断された場合、暗号化部２５４は、ディスク鍵、ディスクＩＤおよび記録情報を作用させて生成された、保護すべきコンテンツ用のブロック鍵を用いて、コンテンツを暗号化する。

また、入出力制御部１２２によりＡＶボード１１２からの入力されたコンテンツが保護不要のコンテンツである（入力されたコンテンツの記録コマンドが、保護不要のコンテンツの記録コマンドである）と判断された場合、暗号化部２５４は、少なくともＲＫＢにより作成されたディスク鍵を作用させて生成された、保護不要のコンテンツ用のブロック鍵を用いて、コンテンツを暗号化する。ＲＫＢにより作成されたディスク鍵を作用させるのは、不正なドライブを排除するようにするためである。なお、これらの保護すべきコンテンツ用および保護不要のコンテンツ用のブロック鍵は、ドライブ１１１に光ディスク１４１が新しく装着される毎に、図２６を参照して後述するブロック鍵生成処理により予め作成され、暗号化部２５４に内蔵されるメモリ（図示せず）に記憶されている。

次に、図２６のフローチャートを参照して、図２４のコンテンツ保護部４１１のブロック鍵生成処理を説明する。

ステップＳ２４１において、記録再生処理部１２３は、ドライブ１１１に新しく光ディスク１４１が装着されるまで待機しており、ステップＳ２４１において、光ディスク１４１が装着されたと判断した場合、ステップＳ２４２において、記録再生処理部１２３は、光ディスク１４１に記録されているディスクＩＤおよびＲＫＢ（ディスク情報）を再生し、コンテンツ保護部４１１に供給する。

ステップＳ２４３において、ＲＫＢ処理部２５２は、供給されたＲＫＢと内蔵するメモリに予め記憶されているデバイスＩＤおよびデバイスキーを用いて、ディスク鍵を取得する。なお、この処理は、図１６のステップＳ１２３の処理と同様であるため、その説明は繰り返しになるので省略する。

ステップＳ２４４において、鍵生成部２５３は、記録再生処理部１２３より供

給されたディスクＩＤ、ステップＳ２４３において生成されたディスク鍵、および、コンテンツ保護部４１１の記録情報などを作用させて、保護すべきコンテンツ用のブロック鍵を生成し、暗号化部２５４に内蔵されるメモリなどに記憶する。

ステップＳ２４５において、鍵生成部２５３は、少なくとも、ステップＳ２４３において生成されたディスク鍵を作用させて、保護不要のコンテンツ用のブロック鍵を生成し、暗号化部２５４に内蔵されるメモリなどに記憶する。

以上のように、図２４のコンテンツ保護部４１１においては、光ディスク１４１が装着されるたびに、保護すべきコンテンツ用および保護不要のコンテンツ用の２種類のブロック鍵が生成され、記憶される。なお、上記説明においては、ブロック鍵を生成したが、ブロック鍵を生成するためのディスクＩＤ、ディスク鍵などを記憶しておき、暗号化する際に、そのコンテンツの保護状態に応じて、ブロック鍵を生成するようにしてもよい。

次に、図２７のフローチャートを参照して、図２４のＡＶボード１１２の記録要求処理を説明する。なお、図２７の記録要求処理は、図１５の記録要求処理のステップＳ１０３およびＳ１０４が除かれている点を除き、図１５の記録要求処理を同様の処理である。

したがって、ドライブ１１１においては、相互認証され、共通鍵が、ＡＶボード１１２と共有されている状態において、それ以降の処理が実行される。

ステップＳ２６１において、ＡＶコンテンツ処理部１３３によりコンテンツが入力される。ステップＳ２６２において、ＡＶコンテンツ処理部１３３により保護すべきコンテンツであると判断された場合、ステップＳ２６３において、そのコンテンツが、相互認証部１３１により、ドライブ１１１との共通鍵を用いて暗号化される。ステップＳ２６４において、暗号化されたコンテンツがドライブ１１１に出力される。ステップＳ２６２において、保護不要のコンテンツであると判断されると、暗号化せず（ステップＳ２６３の処理はスキップされ）、ステップＳ２６４において、ドライブ１１１に出力される。

以上のようにして、ＡＶボード１１２からは、保護すべきコンテンツがドライ

ブ１１１との共通鍵を用いて暗号化され、出力される。また、保護不要のコンテンツは、そのまま出力される。これに対応して実行される図２４のドライブ１１１の記録処理を、図２８のフローチャートを参照して説明する。なお、図２８のステップＳ３０１乃至Ｓ３０４、ステップＳ３０６およびＳ３０７、並びにステップＳ３０９およびＳ３１０は、図１８のステップＳ１６１乃至Ｓ１６８と同様の処理であるため、その詳細な説明は省略する。

ステップＳ３０１において、ドライブ１１１の相互認証部１２１は、バス１１３を介して、ＡＶボード１１２よりコンテンツを受信する。

ステップＳ３０２において、入出力制御部１２２は、相互認証部１２１からの情報に基づいて、このコンテンツを入力してきたＡＶボード１１２が、ドライブ１１１において相互認証されているか否かを判断し、ＡＶボード１１２が、ドライブ１１１において相互認証されていると判断された場合、ステップＳ３０３において、入出力制御部１２２は、相互認証部１２１に入力されたコンテンツが共通鍵により暗号化されているか否かに基づいて、入力されたコンテンツの記録コマンドが、バス１１３上で保護すべきコンテンツの記録コマンドであるかを判断する。

ステップＳ３０３において、入力されたコンテンツの記録コマンドが、バス１１３上で保護すべきコンテンツの記録コマンドであると判断された場合、ステップＳ３０４において入出力制御部１２２は、相互認証部１２１を制御し、受信したコンテンツを、ＡＶボード１１２との共通鍵で復号させ、そのコンテンツをコンテンツ保護部４１１に供給させる。

ステップＳ３０５において、暗号化部２５４は、供給されたコンテンツを、保護すべきコンテンツ用のブロック鍵を用いて暗号化する。この保護すべきコンテンツ用のブロック鍵は、図２６を参照して上述したように、暗号化部２５４のメモリ内に予め記憶されている。そして、入出力制御部１２２は、記録再生処理部１２３を制御し、ステップＳ３０６において、このコンテンツに対応するユーザコントロールデータのＵＣ（０，Ｓ）に、バス１１３上で保護すべきコンテンツ

であるという保護情報「０」を生成、格納させ、ステップＳ３１０において、保護すべきコンテンツ用のブロック鍵を用いて暗号化されたコンテンツとともに、光ディスク１４１に記録させる。

一方、例えば、相互認証部を有しないＨＤＤ１１４に記憶されているコンテンツが入力される。このとき、ステップＳ３０１において、ＨＤＤ１１４からのコンテンツが、バス１１３を介して相互認証部１２１に受信される。ステップＳ３０２において、コンテンツを入力してきた装置がドライブ１１１において相互認証されていないと判断される。ステップＳ３０７において、入出力制御部１２２により、相互認証部１２１に入力されたコンテンツが共通鍵で暗号化されているか否かに基づいて、入力されたコンテンツの記録コマンドが、バス１１３上で保護すべきコンテンツの記録コマンドであるか否かが判断される。

ステップＳ３０３において、または、ステップＳ３０７において、入力されたコンテンツの記録コマンドが、バス１１３上で保護不要のコンテンツの記録コマンドであると判断された場合、ステップＳ３０８において、暗号化部２５４は、相互認証部１２１より供給されたコンテンツを、保護不要のコンテンツ用のブロック鍵を用いて暗号化する。この保護不要のコンテンツ用のブロック鍵は、図２６を参照して上述したように、暗号化部２５４のメモリ内に予め記憶されている。

ステップＳ３０９において、入出力制御部１２２は、記録再生処理部１２３を制御し、コンテンツに対応するユーザコントロールデータのＵＣ（０，Ｓ）に、バス１１３上で保護不要のコンテンツであるという保護情報「１」を生成、格納させ、ステップＳ３１０において、生成された保護情報を、コンテンツとともに、光ディスク１４１に記録させる。

また、ステップＳ３０７において、入力されたコンテンツの記録コマンドが、バス１１３上で保護すべきコンテンツの記録コマンドであると判断された場合、エラーとなり、ドライブ１１１の記録処理は、強制的に終了される。

以上のようにして、相互認証されているＡＶボード１１２からの保護すべきコンテンツは、ディスクＩＤおよびＲＫＢを作用させたブロック鍵で暗号化され、

バス１１３上で保護すべきコンテンツであるという保護情報「０」とともに光ディスク１４１に記録される。また、相互認証されているＡＶボード１１２からの保護不要のコンテンツ、または、相互認証されていないＨＤＤ１１４からの保護不要のコンテンツは、ＲＫＢのみを作用させたブロック鍵で暗号化され、バス１１３上で保護不要のコンテンツであるという保護情報「１」とともに光ディスク１４１に記録される。さらに、相互認証されていないＨＤＤ１１４からの保護すべきコンテンツは、光ディスク１４１には、記録されない。

次に、図２９のフローチャートを参照して、図２４のドライブ１１１のコンテンツ再生処理について説明する。なお、図２９のステップＳ３２１乃至Ｓ３２５、並びにステップＳ３２７乃至Ｓ３３０は、図１９のステップＳ１９１乃至Ｓ２００と同様の処理であるため、その詳細な説明は省略する。

ユーザは、光ディスク１４１に記録されている保護すべきコンテンツを、ＡＶボード１１２の出力部１３５から出力させるために、操作入力部を介して、ＡＶボード１１２に、コンテンツの再生コマンドを入力する。ＡＶボード１１２の相互認証部１３１は、バス１１３を介して、ドライブ１１１に再生コマンドを送信してくる。ステップＳ３２１において、相互認証部１２１は、ＡＶボード１１２からの再生コマンドを入力する。ステップＳ３２２において、相互認証部１２１からの情報に基づいて、コンテンツを出力するＡＶボード１１２が、ドライブ１１１において相互認証されていると判断された場合、ステップＳ３２３において、入出力制御部１２２により、ＡＶボード１１２からの再生コマンドが、保護すべきコンテンツの再生コマンドであるか否かが判断される。

ステップＳ３２３において、ＡＶボード１１２からの再生コマンドが、保護すべきコンテンツの再生コマンドであると判断された場合、ステップＳ３２４において、記録再生処理部１２３により、光ディスク１４１から指示されたコンテンツが再生される。ステップＳ３２５において、入出力制御部１２２により、そのコンテンツに対応するユーザコントロールデータのＵＣ（０，Ｓ）が「０」であると判断された場合、再生されたコンテンツがバス１１３上で保護すべきコンテ

ンツであるものとされる。ステップＳ３２６において、暗号化部２５４は、内蔵するメモリに記憶された保護すべきコンテンツ用のブロック鍵を用いて、再生されたコンテンツを復号する。ステップＳ３２７において、相互認証部１２１は、暗号化部２５４より供給されたコンテンツを、ＡＶボード１１２との共通鍵を用いて暗号化し、バス１１３を介してＡＶボード１１２に出力する。

一方、例えば、ユーザは、光ディスク１４１に記録されている保護不要のコンテンツを、ＨＤＤ１１４に保存（記録）させるために、操作入力部を介して、ＨＤＤ１１４にコンテンツの再生コマンドを入力する。ＨＤＤ１１４は、バス１１３を介して、ドライブ１１１に再生コマンドを送信してくるので、ステップＳ３２１において、相互認証部１２１は、ＨＤＤ１１４からの再生コマンドを入力する。ステップＳ３２２において、相互認証部１２１からの情報に基づいて、コンテンツを出力するＨＤＤ１１４が、相互認証されていないと判断され、ステップＳ３２８において、ＨＤＤ１１４からの再生コマンドが、保護すべきコンテンツの再生コマンドであるか否かが判断される。

ステップＳ３２３において、または、ステップＳ３２８において、ＨＤＤ１１４からの再生コマンドが、保護不要のコンテンツの再生コマンドであると判断された場合、ステップＳ３２９において、記録再生処理部１２３により指示されたコンテンツが光ディスク１４１から再生され、ステップＳ３３０において、入出力制御部１２２は、そのコンテンツに対応するユーザコントロールデータのＵＣ（０，Ｓ）が「１」であるか否かを判断する。ステップＳ３３０において、入出力制御部１２２によりそのコンテンツに対応するユーザコントロールデータのＵＣ（０，Ｓ）が「１」であると判断された場合、再生されたコンテンツがバス１１３上で保護不要のコンテンツであるとする。ステップＳ３３１において暗号化部２５４は、内蔵するメモリに記憶された保護不要のコンテンツ用のブロック鍵を用いて、復号し、コンテンツをそのまま（生データのまま）、相互認証部１２１およびバス１１３を介して、ＡＶボード１１２またはＨＤＤ１１４に出力する。

また、ステップＳ３２５において、コンテンツに対応するＵＣ（０，Ｓ）が

「０」ではないと判断された場合、ステップＳ３２８において、ＨＤＤ１１４からの再生コマンドが、保護すべきコンテンツの再生コマンドであると判断された場合、または、ステップＳ３３０において、コンテンツに対応するＵＣ（０，Ｓ）が「１」ではないと判断された場合、エラーとなり、ドライブ１１１の記録処理は、強制的に終了される。

以上のようにして、相互認証されているＡＶボード１１２からの再生コマンドに対して、バス１１３上で保護すべきコンテンツは、共通鍵で暗号化され、バス１１３を介して、ＡＶボード１１２に出力され、バス１１３上で保護不要のコンテンツは、そのまま（暗号化させずに）、バス１１３を介して、ＡＶボード１１２に出力される。そして、後述する図３０のステップＳ３６１において、ＡＶボード１１２の相互認証部１３１により受信される。

この図２９のドライブ１１１のコンテンツ再生処理に対応するＡＶボード１１２の再生処理を、図３０のフローチャートを参照して説明する。なお、図３０の再生処理は、図２０の再生処理のステップＳ２０４およびＳ２０５を省略した点を除き、図２０の場合と同様である。

ステップＳ３６１において、相互認証部１３１により、ドライブ１１１からのコンテンツが受信され、ステップＳ３６２において、そのコンテンツが、共通鍵を用いて暗号化されており、保護すべきコンテンツであると判断された場合、ステップＳ３６３において、ドライブ１１１との共通鍵を用いて受信されたコンテンツが復号される。

一方、ステップＳ３６２において、暗号化されておらず、保護不要のコンテンツであると判断された場合、このコンテンツは、暗号化されていないので、復号する必要はない。したがって、相互認証部１３１およびコンテンツ保護部１３２を素通りするため、ステップＳ３６３の処理はスキップされる。

ステップＳ３６４において、ＡＶコンテンツ処理部１３３は、コンテンツ保護部１３２から供給されたコンテンツを、例えば、MPEG 方式でデコードし、再生する。ステップＳ３６５において、出力部１３５は、再生されたコンテンツを出

力する。

以上のようにして、ドライブ１１１と相互認証されているＡＶボード１１２においては、光ディスク１４１に記録されているバス１１３上で保護すべきコンテンツ、および、バス１１３上で保護不要のコンテンツの両方を出力することができる。

図３１は、本発明の記録再生装置の他の構成例を示している。なお、図３１の記録再生装置５０１の基本的な構成は、図２４の記録再生装置４０１と同様であるが、図３１の記録再生装置５０１においては、図２４の記録再生装置４０１におけるドライブ１１１の相互認証部１２１が除かれている。

したがって、図３１の記録再生装置５０１においては、ＡＶボード１１２は、バス１１３上に接続されていても、ドライブ１１１が、相互認証機能を有しないため、ＡＶボード１１２において相互認証されず（共通鍵が共有されず）、ＡＶボード１１２からのコンテンツの再生要求処理は実行されないが、相互認証機能を有しないＨＤＤ１１４との保護不要のコンテンツの送受信処理が実行される。

この記録再生装置５０１のドライブ１１１の記録処理を、図３２のフローチャートを参照して説明する。なお、図３２のステップＳ４０１乃至Ｓ４０５は、図２８のステップＳ３０１およびステップＳ３０７乃至Ｓ３１０と同様の処理であり、その説明は繰り返しになるので適宜省略する。

したがって、ステップＳ４０１において、ＨＤＤ１１４からの保護不要のコンテンツが、バス１１３を介して記録再生処理部１２３に受信され、ステップＳ４０２において、入出力制御部１２２により、相互認証部１２１に入力されたコンテンツが共通鍵で暗号化されているか否かに基づいて、入力されたコンテンツの記録コマンドが、バス１１３上で保護すべきコンテンツの記録コマンドではないと判断される。ステップＳ４０３において、暗号化部２５４により、保護不要のコンテンツ用のブロック鍵を用いて、コンテンツが暗号化される。

ステップＳ４０４において、記録再生処理部１２３により、コンテンツに対応するユーザコントロールデータのＵＣ（０，Ｓ）に、バス１１３上で保護不要の

コンテンツであるという保護情報「１」が生成、格納され、ステップＳ４０５において、ＨＤＤ１１４からの保護不要のコンテンツとともに、光ディスク１４１に記録される。

また、ステップＳ４０２において、共通鍵で暗号化されているコンテンツが入力され、入力されたコンテンツの記録コマンドが、バス１１３上で保護すべきコンテンツの記録コマンドであると判断された場合、エラーとなり、ドライブ１１１の記録処理は、強制的に終了される。なお、共通鍵ではなく別の方法で暗号化されているコンテンツであれば、バス１１３上で保護不要のコンテンツとして処理させることも可能である。

以上のようにして、相互認証機能を有さないＨＤＤ１１４からのバス１１３上で保護不要のコンテンツが光ディスク１４１に記録される。

次に、この記録再生装置５０１のドライブ１１１の再生処理を、図３３のフローチャートを参照して説明する。なお、図３３のステップＳ４２１乃至Ｓ４２５は、図２９のステップＳ３２１およびステップＳ３２８乃至Ｓ３３１と同様の処理であるため、その詳細な説明を省略する。

したがって、例えば、ユーザは、光ディスク１４１に記録されている保護不要のコンテンツを、ＨＤＤ１１４に保存（記録）させるために、操作入力部を介して、ＨＤＤ１１４に、保護不要のコンテンツの再生コマンドを入力する。ＨＤＤ１１４は、バス１１３を介して、ドライブ１１１に再生コマンドを送信してくるので、ステップＳ４２１において、ＨＤＤ１１４からの再生コマンドが入力され、ステップＳ４２２において、ＨＤＤ１１４からの再生コマンドが、保護不要のコンテンツの再生コマンドであると判断された場合、ステップＳ４２３において、記録再生処理部１２３により、光ディスク１４１から指示されたコンテンツが再生される。

ステップＳ４２４において、入出力制御部１２２により、そのコンテンツに対応するユーザコントロールデータのＵＣ（０，Ｓ）が「１」であると判断された場合、再生されたコンテンツがバス１１３上で保護不要のコンテンツであるとさ

れ、ステップＳ４２５において、暗号化部２５４により、保護不要のコンテンツ用のブロック鍵を用いて、復号され、コンテンツが、そのまま（生データのまま）、相互認証部１２１およびバス１１３を介してコンテンツを出力するＡＶボード１１２またはＨＤＤ１１４に出力される。

一方、ステップＳ４２２において、ＨＤＤ１１４からのコマンドが、保護すべきコンテンツの再生コマンドであると判断された場合、または、ステップＳ４２４において、コンテンツに対応するＵＣ（０，Ｓ）が「１」ではないと判断された場合、相互認証されていないＨＤＤ１１４へは、保護すべきコンテンツの出力はできないので、エラーとなり、ドライブ１１１の記録処理は、強制的に終了される。

以上のようにして、ＨＤＤ１１４への再生コマンドに対して、保護情報「１」が再生され、再生された保護不要のコンテンツは、そのまま（暗号化させずに）、バス１１３を介して、ＨＤＤ１４に出力される。したがって、バス１１３上で保護不要のコンテンツは、暗号化もされていないので、ＨＤＤ１４に供給され、記憶されるようにできる。

また、相互認証されないＨＤＤ１４からのコンテンツは、ＨＤＤ１４により保護すべきコンテンツであると示されたとしても、ドライブ１１１においては、保護すべきコンテンツとしては認識されず、保護不要のコンテンツとしてであれば、扱うようにできる。以上のように、コピーフリーのコンテンツのみを扱う相互認証しないストレージ運用が可能になる。

なお、上記説明においては、記録媒体を、光ディスク１４１としたが、記録媒体は、光ディスク１４１だけでなく、光ディスク１４１以外のメモリーカード（登録商標）、その他の記録媒体とすることもできる。

上述した一連の処理は、ハードウェアにより実行させることもできるし、ソフトウェアにより実行させることもできる。この場合、例えば、図４の記録再生装置１０１、図２１の記録再生装置３０１、図２４の記録再生装置４０１および図３１の記録再生装置５０１は、図３４に示されるような記録再生装置６０１によ

り構成される。

図３１において、ＣＰＵ（Central Processing Unit）６１１は、ＲＯＭ(Read Only Memory)６１２に記憶されているプログラム、または、ＨＤＤ６１９からＲＡＭ（Random Access Memory）６１３にロードされたプログラムに従って各種の処理を実行する。ＲＡＭ６１３にはまた、ＣＰＵ６１１が各種の処理を実行する上において必要なデータなどが適宜記憶される。

ＣＰＵ６１１、ＲＯＭ６１２、およびＲＡＭ６１３は、バス６１４を介して相互に接続されている。このバス６１４にはまた、入出力インタフェース６１５も接続されている。

入出力インタフェース６１５には、コンテンツの入出力の制御を行うＡＶボード６１６、キーボード、マウスなどよりなる入力部６１７、ＣＲＴ(Cathode Ray Tube)，ＬＣＤ（Liquid Crystal Display）などよりなるディスプレイ、並びにスピーカなどよりなる出力部６１８、ＨＤＤ６１９、モデム、ターミナルアダプタなどより構成される通信部６２０が接続されている。通信部６２０は、バスや図示しないネットワークを介しての通信処理を行う。

入出力インタフェース６１５にはまた、必要に応じてドライブ６３０が接続され、磁気ディスク６３１、光ディスク６３２、光磁気ディスク６３３、或いは半導体メモリ６３４などが適宜装着され、それから読み出されたコンピュータプログラムが、必要に応じてＨＤＤ６１９にインストールされる。

一連の処理をソフトウェアにより実行させる場合には、そのソフトウェアを構成するプログラムが、専用のハードウェアに組み込まれているコンピュータ、または、各種のプログラムをインストールすることで、各種の機能を実行することが可能な、例えば、汎用のパーソナルコンピュータなどに、ネットワークや記録媒体からインストールされる。

この記録媒体は、図３４に示すように、装置本体とは別に、ユーザにプログラムを提供するために配布される、プログラムが記録されている磁気ディスク６３１（フレキシブルディスクを含む）、光ディスク６３２（CD-ROM(Compact Dis

k-Read Only Memory), DVD(Digital Versatile Disk)を含む）、光磁気ディスク６３３（MD(Mini-Disk)（商標）を含む）、もしくは半導体メモリ６３４などよりなるパッケージメディアにより構成されるだけでなく、装置本体に予め組み込まれた状態でユーザに提供される、プログラムが記録されているＲＯＭ６１２や、ＨＤＤ６１９などで構成される。

なお、コンテンツおよび保護情報などを記録もしくは再生する図４の光ディスク１４１が、例えば、DVD の他、CD-R その他の光ディスク、MD その他の光磁気ディスク、磁気ディスク等のディスク型の記録媒体である場合、ディスク表面に同心円状またはスパイラル状に設定された「トラック」の上に、ピットまたはマークをデータの記録波形に基づいて形成することにより、情報が記録されるようになされている。

例えば、CD-ROM や DVD-ROM など、プレスしてデータを記録するメディアでは、実際に表面に物理的なくぼみであるピットが形成される。これに対し、例えば、CD-R、CD-RW、DVD-R、DVD-RW、または、DVD-RAM などの追記または書き換え型のメディアの場合、物理的なくぼみをつける代わりに、レーザ光を当て、その熱によってメディア内部の相変化膜に化学変化を生じさせることにより、くぼみの代用であるマークが形成される。

記録されたデータが再生される場合、データを読み取るためにヘッドから照射されたレーザ光は、メディア表面で反射するが、その際、このピットまたはマークの有無によって反射光に変化が生じることによりデータが再生される。

記録されているデータの認識方法には、ピットの有無がビットデータを表す「マークポジション記録方式」と、ピットの存在がビットを反転させる「マークエッジ記録方式」が存在する。

後者は、反射率が一定の状態で読み取られたピットを「０」、反射率がピット中で変化したピットを「１」と認識する方式で、データを記録する際のトラックのロスを少なくし、ピット長を縮めることに貢献している。

なお、図３４を参照して上述した磁気ディスク６３１、光ディスク６３２、光

磁気ディスク６３３、ＲＯＭ６１２、または、ＨＤＤ６１９などのディスク型の記録媒体における情報の記録または再生の方法も、図４の光ディスク１４１がディスク型の記録媒体である場合と同様である。

なお、本明細書において、記録媒体に記録されるプログラムを記述するステップは、記載された順序に従って時系列的に行われる処理はもちろん、必ずしも時系列的に処理されなくとも、並列的あるいは個別に実行される処理をも含むものである。

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものである。

産業上の利用可能性

以上の如く、本発明によれば、保護の要不要に基づいて、コンテンツを柔軟に保護することができる。また、本発明によれば、コンテンツの不正コピーが抑制される。さらに、本発明によれば、ＰＣストレージ運用が可能になる。

請求の範囲

1． 入力装置と記録装置がバスを介して接続された記録システムにおいて、

前記入力装置は、入力されたコンテンツを保護するか否かを判断する判断手段を備え、

前記記録装置は、前記判断手段により判断された結果に基づいて、前記コンテンツが前記バス上での伝送において保護すべきコンテンツであるか否かを示す保護情報を、前記コンテンツとともに記録媒体に記録する記録手段を備える

ことを特徴とする記録システム。

2． 前記記録手段は、前記コンテンツの所定の単位ごとに前記保護情報を記録する

ことを特徴とする請求の範囲第１項に記載の記録システム。

3． 前記所定の単位は、２０４８バイトである

ことを特徴とする請求の範囲第２項に記載の記録システム。

4． 前記記録装置は、前記判断手段により前記コンテンツを保護すると判断された場合、前記記録媒体のＩＤと記録媒体鍵を作用させて前記コンテンツを暗号化する暗号化手段をさらに備える

ことを特徴とする請求の範囲第１項に記載の記録システム。

5． 前記記録装置は、前記判断手段により前記コンテンツを保護しないと判断された場合、少なくとも、前記記録媒体の記録媒体鍵を作用させて前記コンテンツを暗号化する暗号化手段をさらに備える

ことを特徴とする請求の範囲第１項に記載の記録システム。

6． 前記入力装置および前記記録装置は、それぞれ相互に認証する認証手段をさらに備える

ことを特徴とする請求の範囲第１項に記載の記録システム。

7． 前記入力装置は、前記判断手段により前記コンテンツを保護すると判断された場合、前記バスへの前記コンテンツの送出前に、前記コンテンツを暗号化する第１の暗号化手段をさらに備え、

前記記録装置は、前記判断手段により前記コンテンツを保護すると判断された場合、前記記録手段による前記コンテンツの記録前に、前記コンテンツを暗号化する第２の暗号化手段をさらに備える

ことを特徴とする請求の範囲第１項に記載の記録システム。

８．　前記判断手段により前記コンテンツを保護しないと判断された場合、前記第１の暗号化手段は、前記バスへの前記コンテンツの送出前に、前記コンテンツを暗号化することを禁止する

ことを特徴とする請求の範囲第７項に記載の記録システム。

９．　入力装置と記録装置がバスを介して接続された記録システムの記録方法において、

前記入力装置は、入力されたコンテンツを保護するか否かを判断し、

前記記録装置は、判断された結果に基づいて、前記コンテンツが前記バス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を、前記コンテンツとともに記録媒体に記録する

ことを特徴とする記録方法。

１０．　記録媒体に情報を記録する記録装置において、

バスを介して接続された他の装置と相互に認証を行う認証手段と、

前記他の装置から前記バスを介して供給される第１の暗号化方法により暗号化されたコンテンツを復号する復号手段と、

前記復号手段により復号された前記コンテンツとともに、前記バス上での伝送において保護すべきコンテンツであることを示す保護情報を、前記記録媒体に記録する記録手段と

を備えることを特徴とする記録装置。

１１．　前記復号された前記コンテンツを、第２の暗号化方法により暗号化する暗号化手段をさらに備える

ことを特徴とする請求の範囲第１０項に記載の記録装置。

１２．　前記暗号化手段は、前記記録媒体のＩＤと記録媒体鍵を作用させて前記

復号されたコンテンツを暗号化する

ことを特徴とする請求の範囲第１１項に記載の記録装置。

１３．　前記記録手段は、前記他の装置から前記バスを介して供給された前記コンテンツが、前記第１の暗号方法により暗号化されていないコンテンツの場合、前記コンテンツを、前記バス上での伝送において保護すべきコンテンツでないことを示す保護情報とともに記録する

ことを特徴とする請求の範囲第１０項に記載の記録装置。

１４．　記録媒体に情報を記録する記録装置の記録方法において、

バスを介して接続された他の装置と相互に認証を行う認証ステップと、

前記他の装置から前記バスを介して供給される暗号化されたコンテンツを復号する復号ステップと、

前記復号ステップの処理により復号された前記コンテンツとともに、前記バス上での伝送において保護すべきコンテンツであることを示す保護情報を、前記記録媒体に記録する記録ステップと

を含むことを特徴とする記録方法。

１５．　記録媒体に情報を記録する記録装置用のプログラムであって、

バスを介して接続された他の装置と相互に認証を行う認証ステップと、

前記他の装置から前記バスを介して供給される暗号化されたコンテンツを復号する復号ステップと、

前記復号ステップの処理により復号された前記コンテンツとともに、前記バス上での伝送において保護すべきコンテンツであることを示す保護情報を、前記記録媒体に記録する記録ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

１６．　記録媒体に情報を記録する記録装置のプログラムであって、

バスを介して接続された他の装置と相互に認証を行う認証ステップと、

前記他の装置から前記バスを介して供給される暗号化されたコンテンツを復号

する復号ステップと、

前記復号ステップの処理により復号された前記コンテンツとともに、前記バス上での伝送において保護すべきコンテンツであることを示す保護情報を、前記記録媒体に記録する記録ステップと

を含むことを特徴とするプログラム。

１７．　コンテンツが入力される入力装置において、

バスを介して接続された記録装置と相互に認証を行う認証手段と、

入力された前記コンテンツが前記バス上での伝送において保護すべきコンテンツであるか否かに応じて、前記コンテンツを第１の暗号化方法で暗号化する第１の暗号化手段と、

前記第１の暗号化手段により暗号化された前記コンテンツを、前記バスを介して前記記録装置に供給する供給手段と

を備えることを特徴とする入力装置。

１８．　前記第１の暗号化手段により暗号化された前記コンテンツを、第２の暗号化方法で暗号化する第２の暗号化手段を

さらに備えることを特徴とする請求の範囲第１７項に記載の入力装置。

１９．　前記第１の暗号化手段および前記第２の暗号化手段のうちの一方は、記録媒体のＩＤと記録媒体鍵を作用させて前記コンテンツを暗号化する

ことを特徴とする請求の範囲第１８項に記載の入力装置。

２０．　コンテンツが入力される入力装置の入力方法において、

バスを介して接続された記録装置と相互に認証を行う認証ステップと、

入力された前記コンテンツが前記バス上での伝送において保護すべきコンテンツであるか否かに応じて、前記コンテンツを暗号化する暗号化ステップと、

前記暗号化ステップの処理により暗号化された前記コンテンツを、前記バスを介して前記記録装置に供給する供給ステップと

を含むことを特徴とする入力方法。

２１．　コンテンツが入力される入力装置用のプログラムであって、

バスを介して接続された記録装置と相互に認証を行う認証ステップと、

入力された前記コンテンツが前記バス上での伝送において保護すべきコンテンツであるか否かに応じて、前記コンテンツを暗号化する暗号化ステップと、

前記暗号化ステップの処理により暗号化された前記コンテンツを、前記バスを介して前記記録装置に供給する供給ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

２２．　コンテンツが入力される入力装置のプログラムであって、

バスを介して接続された記録装置と相互に認証を行う認証ステップと、

入力された前記コンテンツが前記バス上での伝送において保護すべきコンテンツであるか否かに応じて、前記コンテンツを暗号化する暗号化ステップと、

前記暗号化ステップの処理により暗号化された前記コンテンツを、前記バスを介して前記記録装置に供給する供給ステップと

を含むことを特徴とするプログラム。

２３．　再生装置と出力装置がバスを介して接続された再生システムにおいて、

前記再生装置は、記録媒体からコンテンツ、および前記コンテンツが前記バス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生手段と、

前記再生手段により再生された前記保護情報に基づいて、前記バス上の前記出力装置への前記コンテンツの送出を制御する送出制御手段とを備え、

前記出力装置は、前記送出制御手段により送出された前記コンテンツを外部に出力する出力手段を備える

ことを特徴とする再生システム。

２４．　前記保護情報は、前記コンテンツの所定の単位ごとに記録されている

ことを特徴とする請求の範囲第２３項に記載の再生システム。

２５．　前記所定の単位は、２０４８バイトである

ことを特徴とする請求の範囲第２４項に記載の再生システム。

２６．　前記再生装置は、前記再生手段により再生されたコンテンツを復号する復号手段をさらに備える

ことを特徴とする請求の範囲第２３項に記載の再生システム。

２７．　前記再生装置は、前記バス上の装置を認証する認証手段をさらに備える

ことを特徴とする請求の範囲第２３項に記載の再生システム。

２８．　前記再生装置は、前記保護情報により前記コンテンツが前記バス上の伝送において保護すべきコンテンツであることが示され、かつ、前記認証手段により前記バス上の前記出力装置が認証されている場合、前記バスへの前記コンテンツの送出前に、前記コンテンツを暗号化する暗号化手段をさらに備え、

前記出力装置は、前記暗号化手段により暗号化された前記コンテンツを復号する第１の復号手段をさらに備える

ことを特徴とする請求の範囲第２７項に記載の再生システム。

２９．　前記出力装置は、前記第１の復号手段により復号された前記コンテンツを、前記記録媒体のＩＤと記録媒体鍵を作用させて復号する第２の復号手段をさらに備える

ことを特徴とする請求の範囲第２８項に記載の再生システム。

３０．　前記保護情報により前記コンテンツが前記バス上の伝送において保護すべきコンテンツであることが示され、かつ、前記認証手段により前記バス上の装置が認証されていない場合、前記送出制御手段は、前記バス上の装置への前記コンテンツの送出を禁止する

ことを特徴とする請求の範囲第２７項に記載の再生システム。

３１．　再生装置と出力装置がバスを介して接続された再生システムの再生方法において、

前記再生装置は、記録媒体からコンテンツ、および前記コンテンツが前記バス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生し、再生された前記保護情報に基づいて、前記バス上の前記出力装置への前記コンテンツの送出を制御し、

前記出力装置は、前記再生装置から送出された前記コンテンツを外部に出力する

ことを特徴とする再生方法。

３２．　コンテンツを記録媒体から再生し、他の装置にバスを介して供給する再生装置において、

前記記録媒体から前記コンテンツ、および前記コンテンツが前記バス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生手段と、

前記再生手段により再生された前記保護情報に基づいて、前記バスを介しての前記他の装置への前記コンテンツの出力を制御する出力制御手段と

を備えることを特徴とする再生装置。

３３．　前記保護情報は、前記コンテンツの所定の単位ごとに記録されている

ことを特徴とする請求の範囲第３２項に記載の再生装置。

３４．　前記所定の単位は、２０４８バイトである

ことを特徴とする請求の範囲第３３項に記載の再生装置。

３５．　前記他の装置を認証する認証手段と、

前記コンテンツを暗号化する暗号化手段とをさらに備え、

前記保護情報により前記コンテンツが前記バス上の伝送において保護すべきコンテンツであることが示され、かつ、前記認証手段により前記他の装置が認証されている場合、前記暗号化手段は、前記バスへの前記コンテンツの送出前に、前記コンテンツを暗号化する

ことを特徴とする請求の範囲第３２項に記載の再生装置。

３６．　前記保護情報により前記コンテンツが前記バス上の伝送において保護すべきコンテンツであることが示され、かつ、前記認証手段により前記他の装置が認証されていない場合、前記出力制御手段は、前記バスへの前記コンテンツの出力を禁止する

ことを特徴とする請求の範囲第３５項に記載の再生装置。

３７．　コンテンツを記録媒体から再生し、他の装置にバスを介して供給する再生装置の再生方法において、

前記記録媒体から前記コンテンツ、および前記コンテンツが前記バス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生ステップと、

前記再生ステップの処理により再生された前記保護情報に基づいて、前記バスを介しての前記他の装置への前記コンテンツの出力を制御する出力制御ステップと

を含むことを特徴とする再生方法。

３８．　コンテンツを記録媒体から再生し、他の装置にバスを介して供給する再生装置用のプログラムであって、

前記記録媒体から前記コンテンツ、および前記コンテンツが前記バス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生ステップと、

前記再生ステップの処理により再生された前記保護情報に基づいて、前記バスを介しての前記他の装置への前記コンテンツの出力を制御する出力制御ステップと

を含むことを特徴とするコンピュータが読み取り可能なプログラムが記録されている記録媒体。

３９．　コンテンツを記録媒体から再生し、他の装置にバスを介して供給する再生装置のプログラムにおいて、

前記記録媒体から前記コンテンツ、および前記コンテンツが前記バス上の伝送において保護すべきコンテンツであるか否かを示す保護情報を再生する再生ステップと、

前記再生ステップの処理により再生された前記保護情報に基づいて、前記バスを介しての前記他の装置への前記コンテンツの出力を制御する出力制御ステップと

を含むことを特徴とするプログラム。

図１

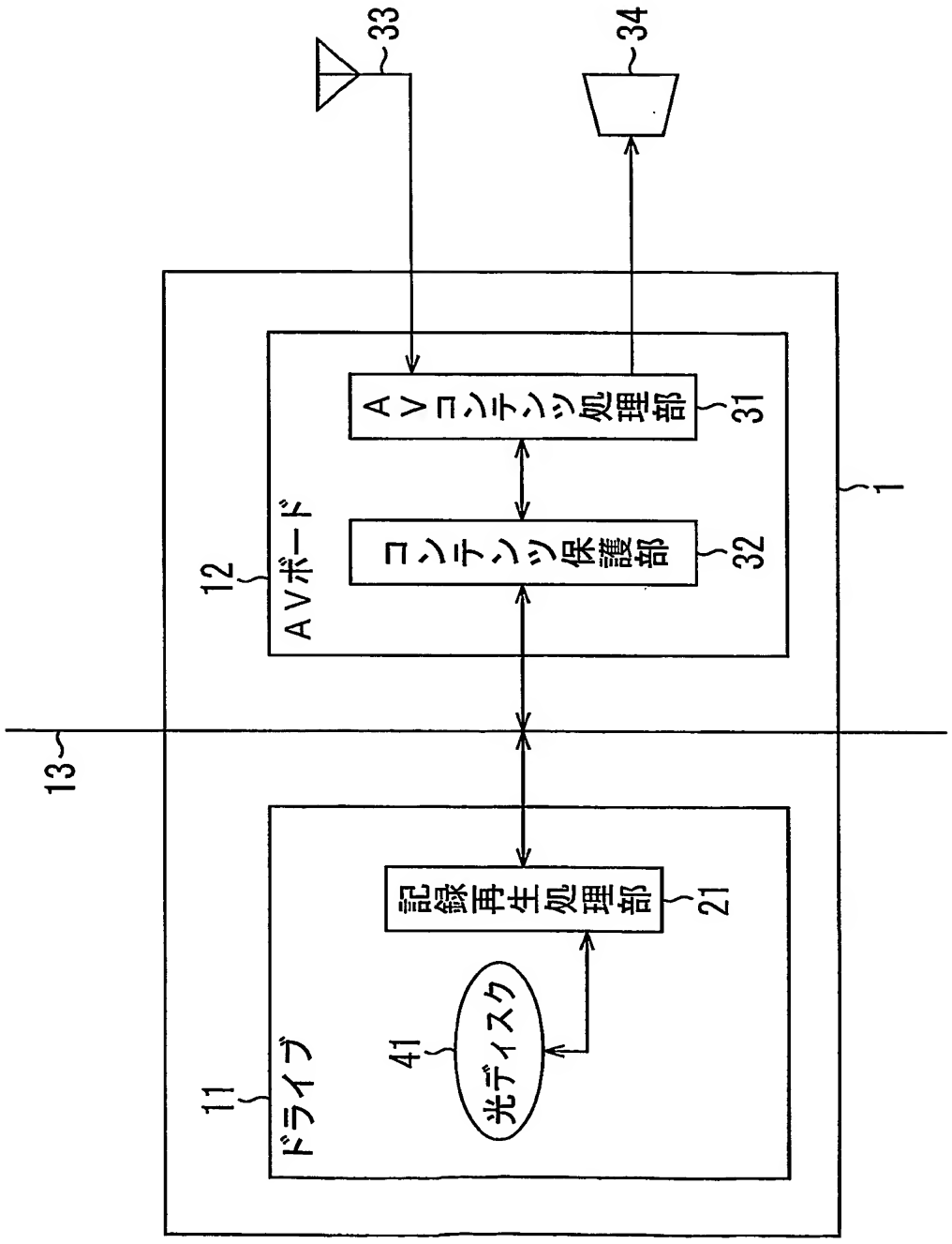

33
34
AVコンテンツ処理部
31
コンテンツ保護部
32
12
AVボード
1
13
記録再生処理部
21
41
光ディスク
11
ドライブ

図2

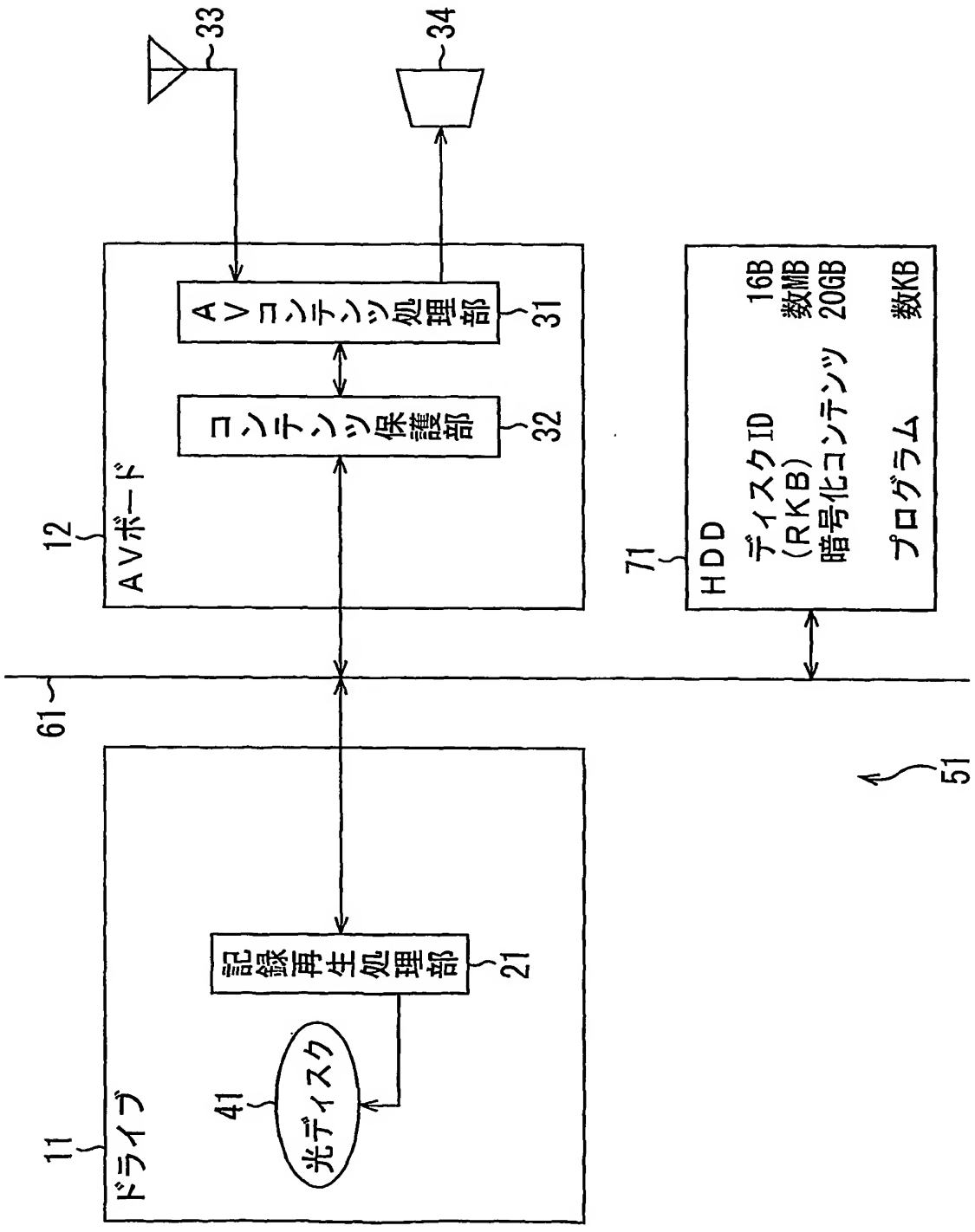

33
34
AVコンテンツ処理部
31
コンテンツ保護部
32
12
AVボード
71
HDD
ディスクID 16B
(RKB) 数MB
暗号化コンテンツ 20GB
プログラム 数KB
61
51
記録再生処理部
21
41
光ディスク
11
ドライブ

図3

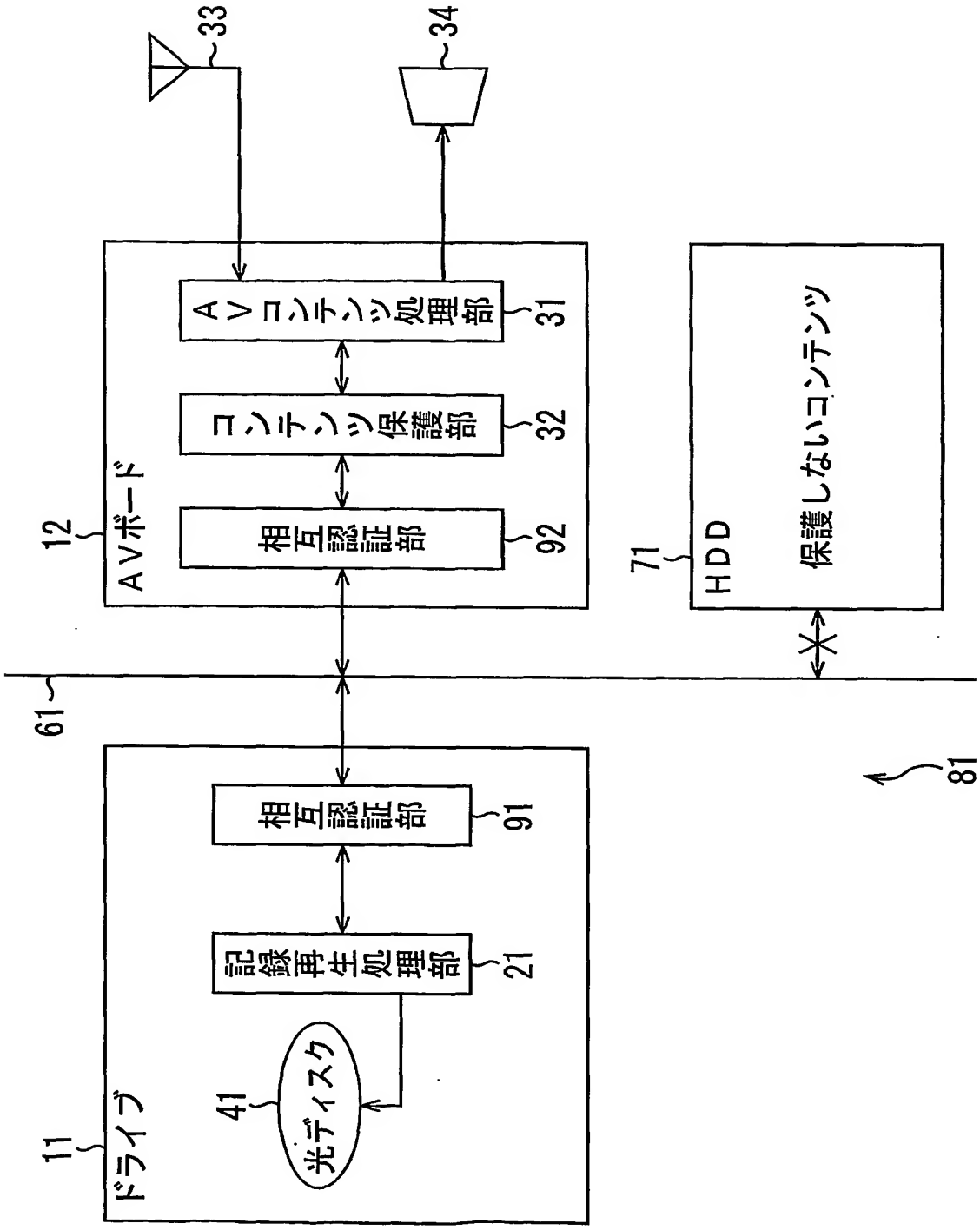

33
34
AVコンテンツ処理部
31
コンテンツ保護部
32
相互認証部
92
12
AVボード
71
HDD
保護しないコンテンツ
61
81
相互認証部
91
記録再生処理部
21
41
光ディスク
11
ドライブ

図４

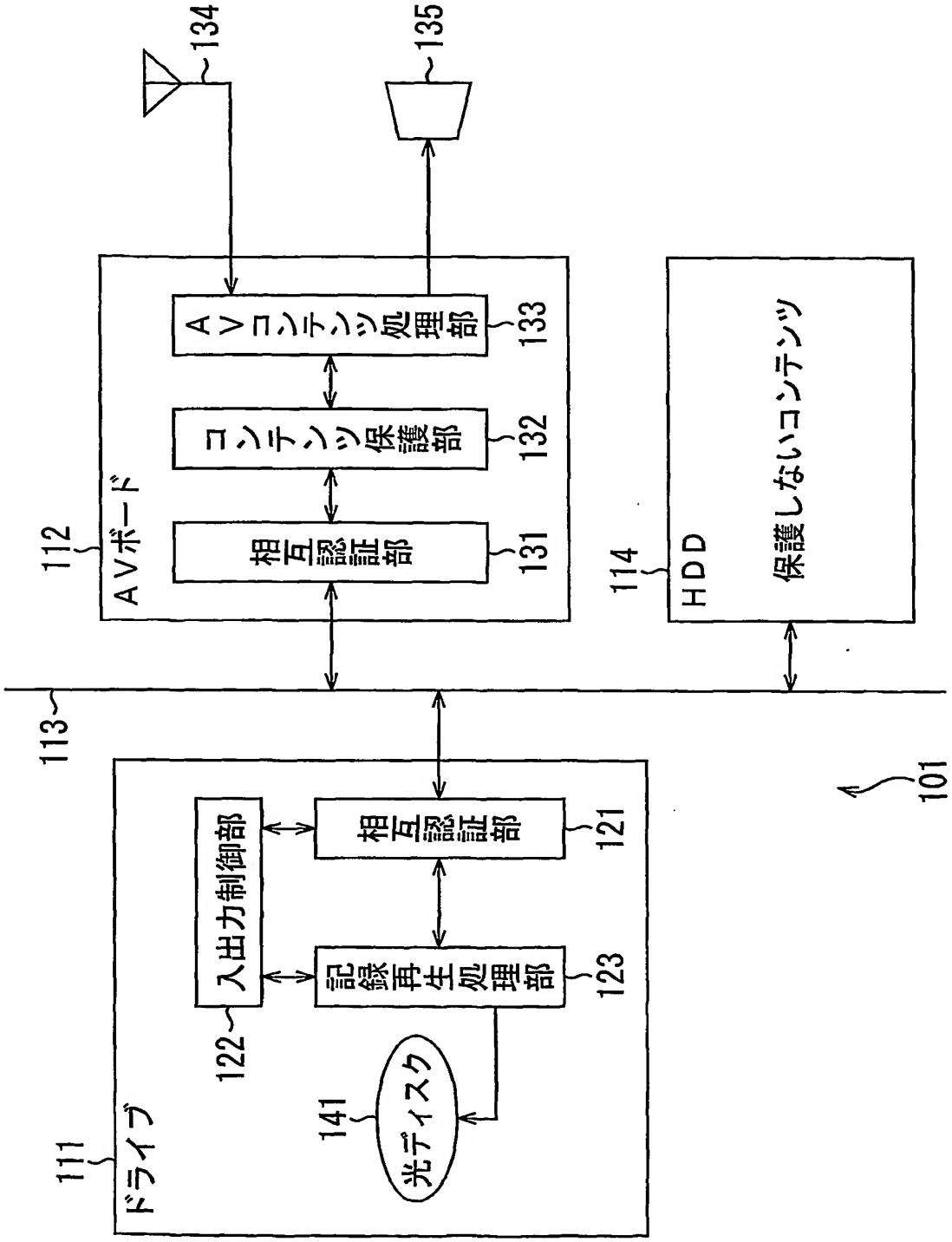

134
135
AVコンテンツ処理部
133
コンテンツ保護部
132
相互認証部
131
112
AVボード
114
HDD
保護しないコンテンツ
113
101
相互認証部
121
入出力制御部
122
記録再生処理部
123
141
光ディスク
111
ドライブ

図５

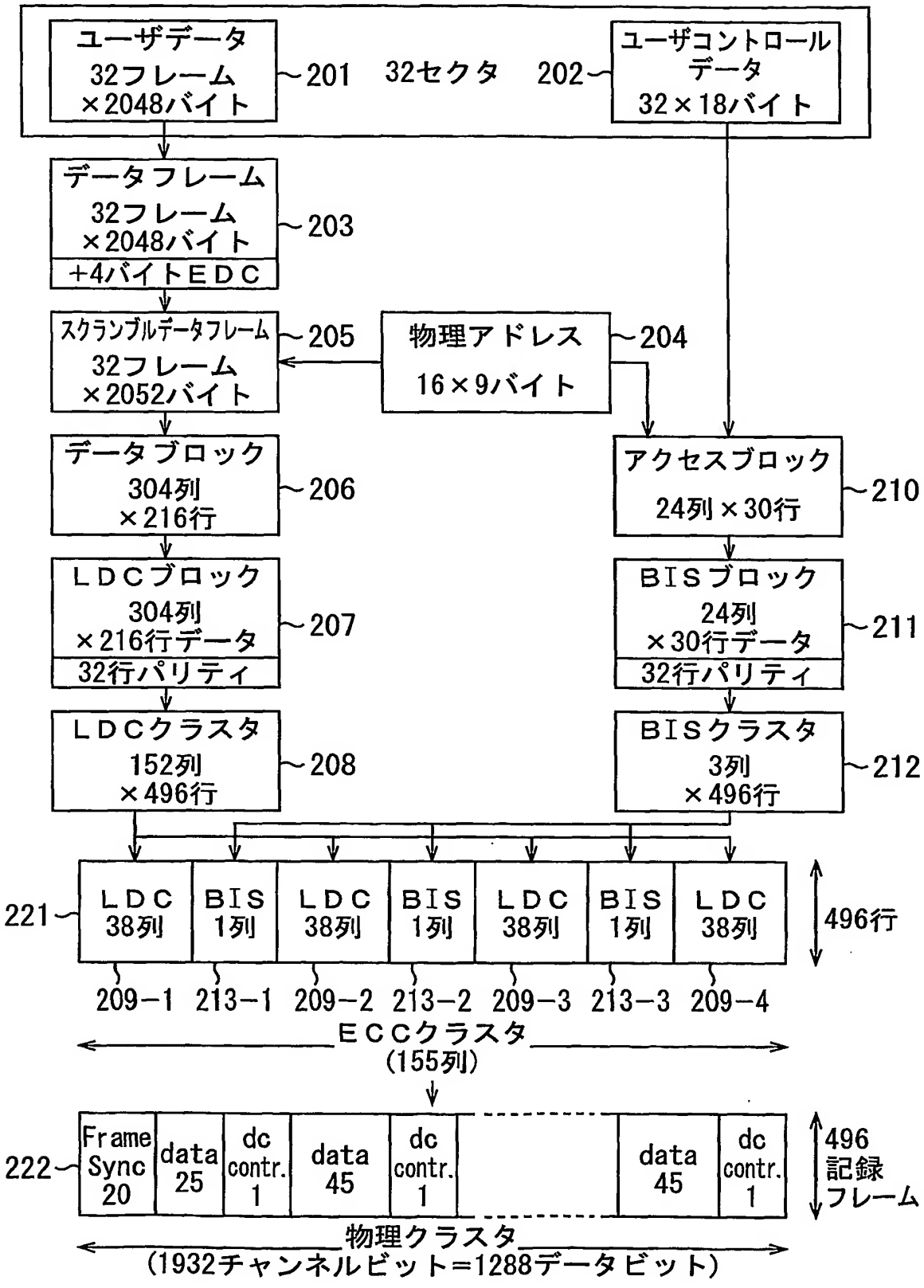

ユーザデータ
32フレーム
×2048バイト
201
32セクタ
202
ユーザコントロールデータ
32×18バイト
データフレーム
32フレーム
×2048バイト
+4バイトＥＤＣ
203
スクランブルデータフレーム
32フレーム
×2052バイト
205
物理アドレス
16×9バイト
204
データブロック
304列
×216行
206
アクセスブロック
24列×30行
210
ＬＤＣブロック
304列
×216行データ
32行パリティ
207
ＢＩＳブロック
24列
×30行データ
32行パリティ
211
ＬＤＣクラスタ
152列
×496行
208
ＢＩＳクラスタ
3列
×496行
212
221
ＬＤＣ 38列
ＢＩＳ 1列
ＬＤＣ 38列
ＢＩＳ 1列
ＬＤＣ 38列
ＢＩＳ 1列
ＬＤＣ 38列
496行
209−1 213−1 209−2 213−2 209−3 213−3 209−4
ＥＣＣクラスタ
(155列)
222
Frame Sync 20
data 25
dc contr. 1
data 45
dc contr. 1
data 45
dc contr. 1
496 記録フレーム
物理クラスタ
(1932チャンネルビット=1288データビット)

図６

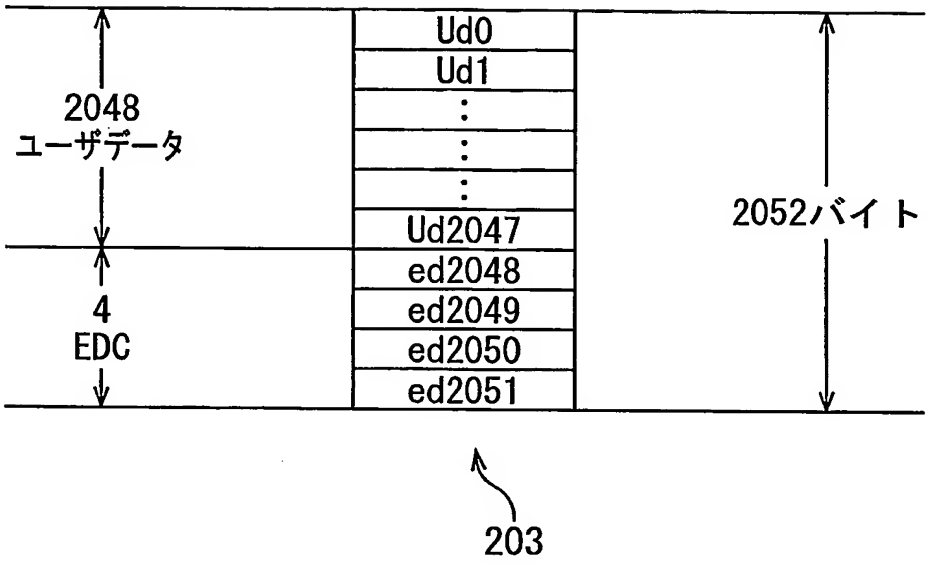

2048
ユーザデータ
4
EDC
Ud0
Ud1
Ud2047
ed2048
ed2049
ed2050
ed2051
2052バイト
203

図７

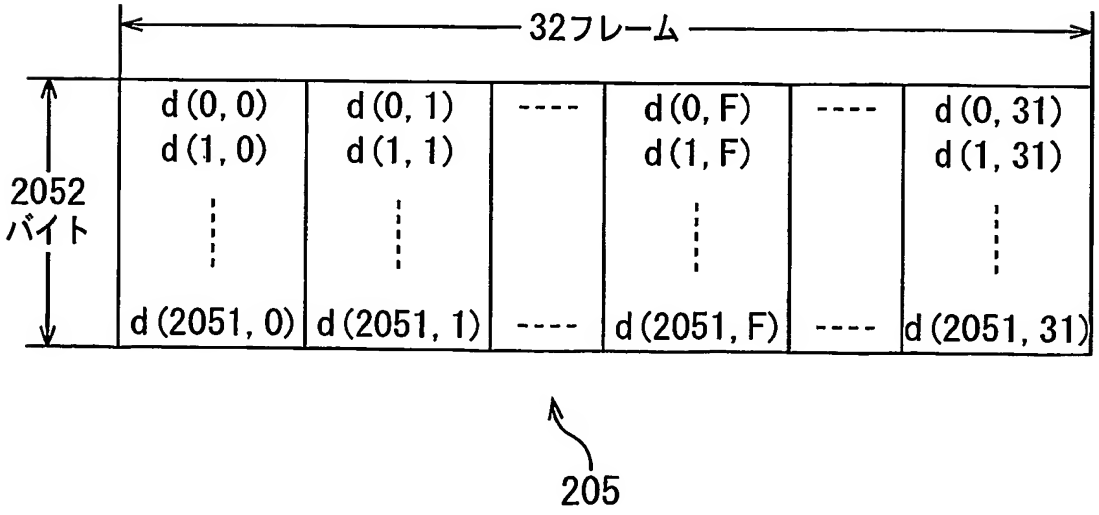
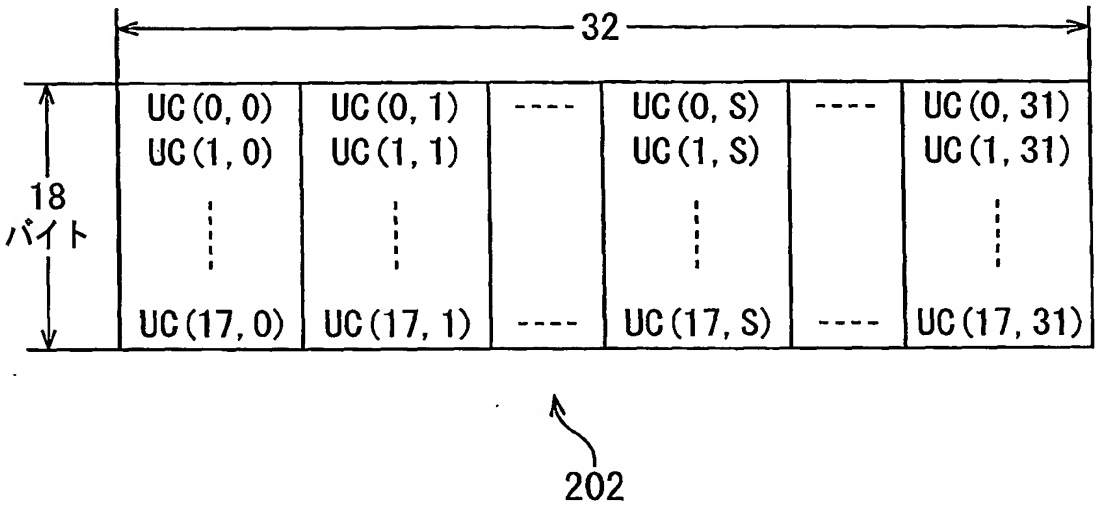

32フレーム
2052
バイト
d (0, 0)
d (1, 0)
d (2051, 0)
d (0, 1)
d (1, 1)
d (2051, 1)
----
d (0, F)
d (1, F)
d (2051, F)
d (0, 31)
d (1, 31)
d (2051, 31)
205

図８


32
18
バイト
UC(0, 0)
UC(1, 0)
UC(17, 0)
UC(0, 1)
UC(1, 1)
UC(17, 1)

UC(0, S)
UC(1, S)
UC(17, S)

UC(0, 31)
UC(1, 31)
UC(17, 31)
202

図9

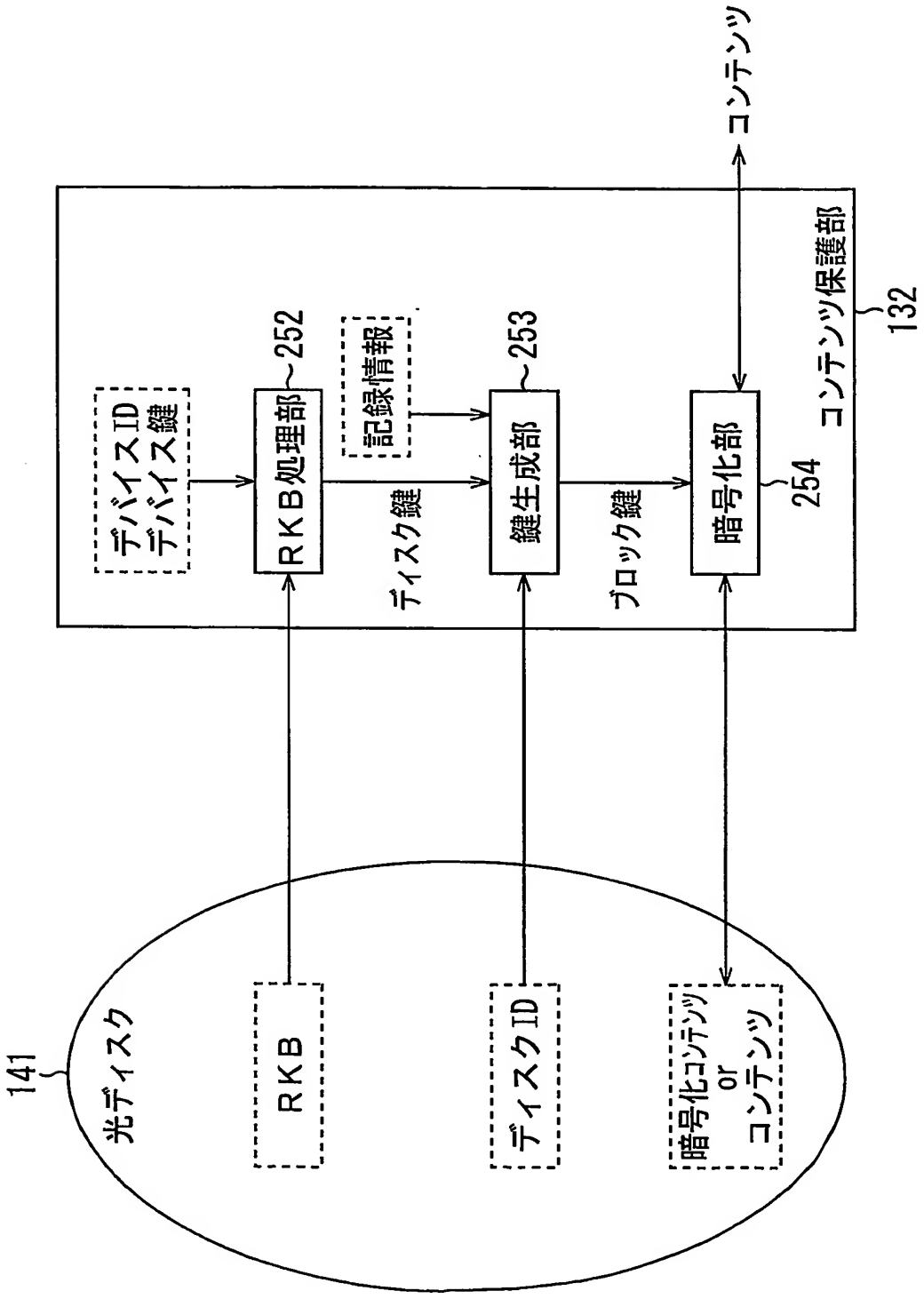

141
光ディスク
RKB
ディスクID
暗号化コンテンツ
or
コンテンツ
デバイスID
デバイス鍵
RKB処理部
252
記録情報
ディスク鍵
鍵生成部
253
ブロック鍵
暗号化部
254
コンテンツ保護部
132
コンテンツ

図10

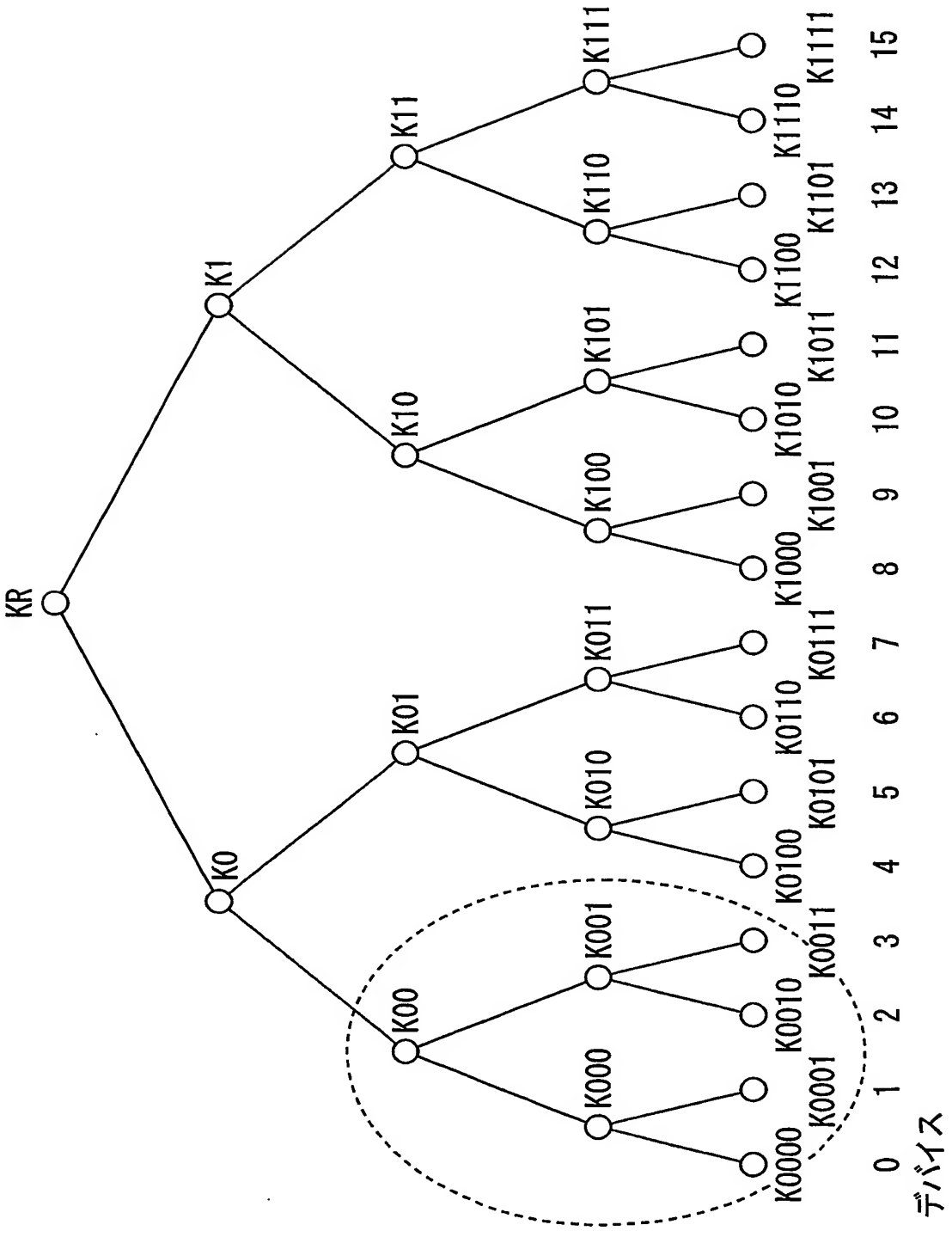

KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
デバイス

図11A

バージョン(Version):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

図11B

バージョン(Version):t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

図12

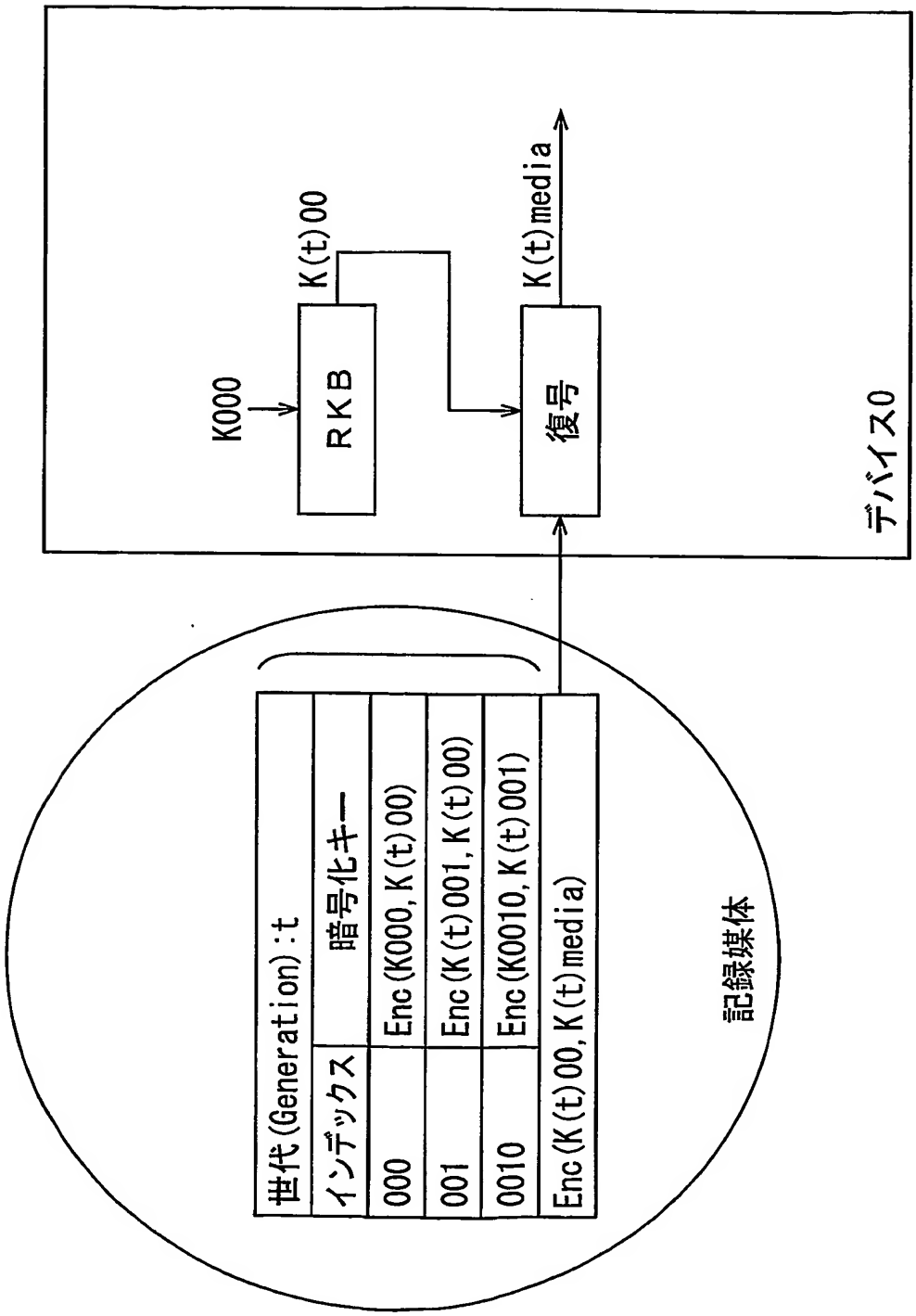

デバイス0
K000
RKB
K(t)00
復号
K(t)media
記録媒体
世代(Generation):t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)media)

図13

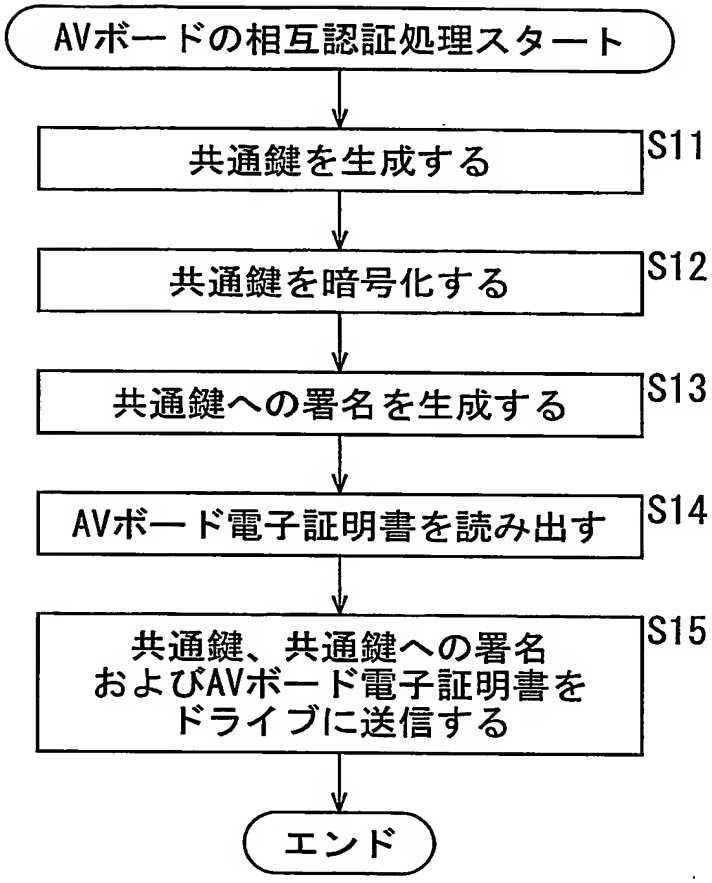

AVボードの相互認証処理スタート
共通鍵を生成する
S11
共通鍵を暗号化する
S12
共通鍵への署名を生成する
S13
AVボード電子証明書を読み出す
S14
共通鍵、共通鍵への署名
およびAVボード電子証明書を
ドライブに送信する
S15
エンド

図14

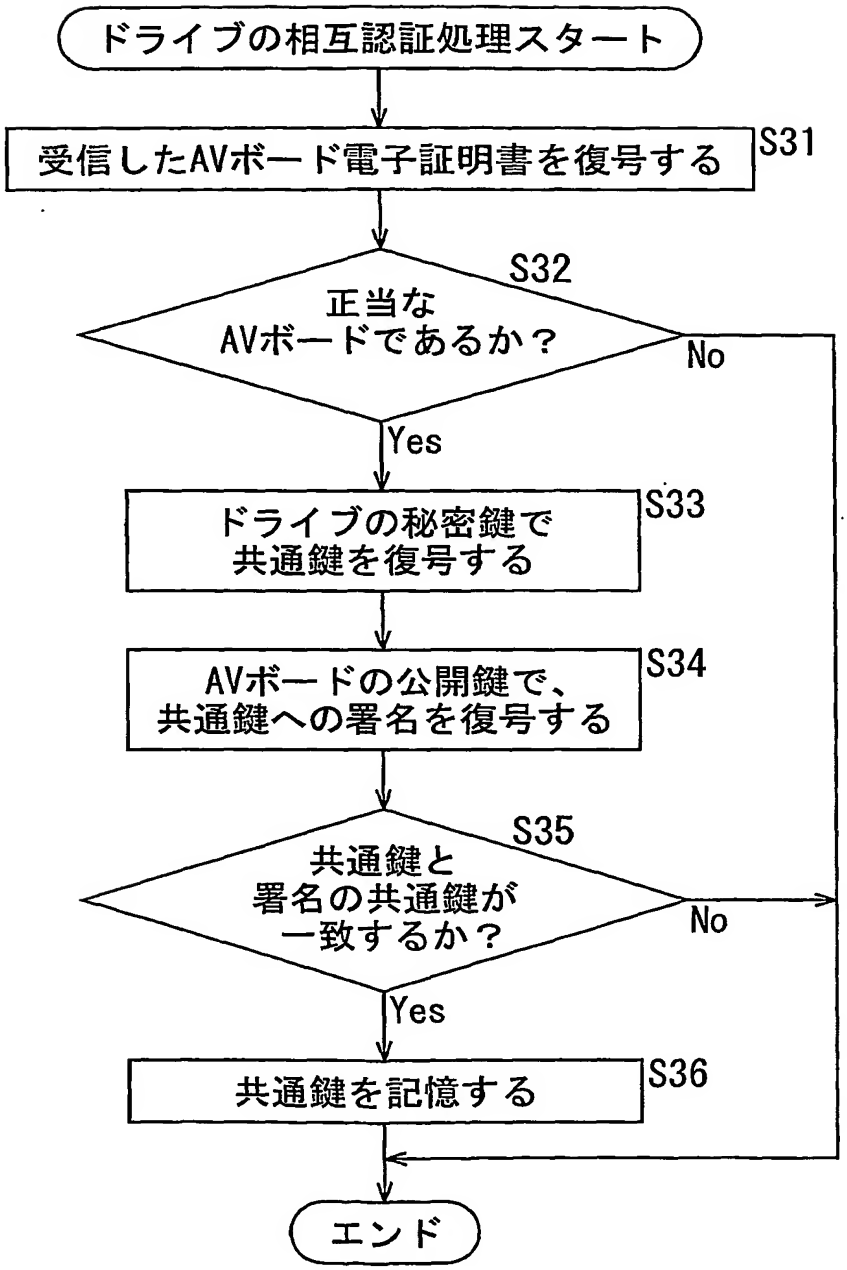

ドライブの相互認証処理スタート
受信したAVボード電子証明書を復号する
S31
S32
正当な
AVボードであるか？
No
Yes
ドライブの秘密鍵で
共通鍵を復号する
S33
AVボードの公開鍵で、
共通鍵への署名を復号する
S34
S35
共通鍵と
署名の共通鍵が
一致するか？
No
Yes
共通鍵を記憶する
S36
エンド

図15

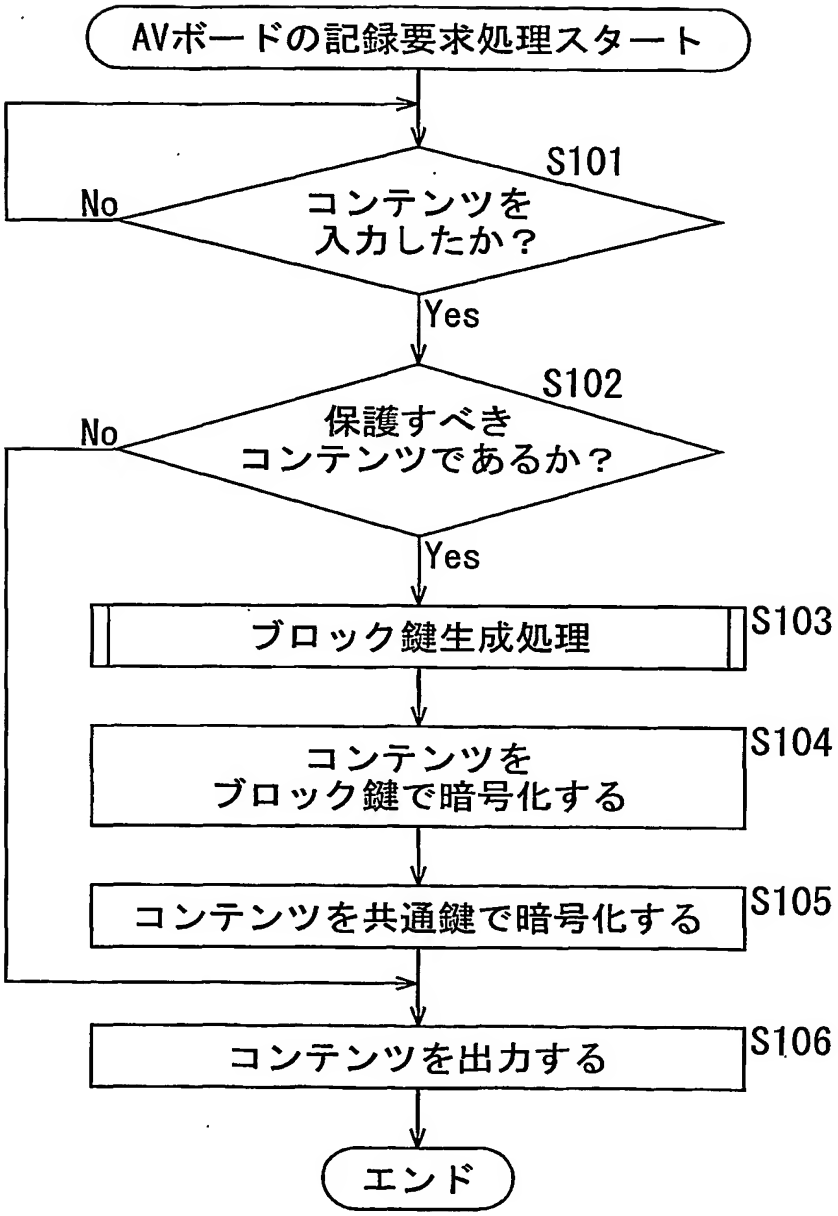

AVボードの記録要求処理スタート
S101
コンテンツを
入力したか？
No
Yes
S102
保護すべき
コンテンツであるか？
No
Yes
ブロック鍵生成処理
S103
コンテンツを
ブロック鍵で暗号化する
S104
コンテンツを共通鍵で暗号化する
S105
コンテンツを出力する
S106
エンド

図16

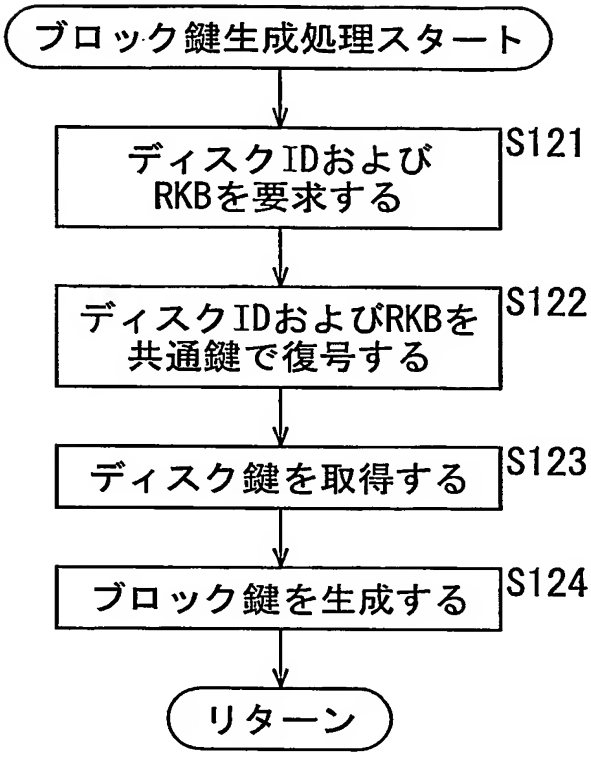

ブロック鍵生成処理スタート
ディスクIDおよび
RKBを要求する
S121
ディスクIDおよびRKBを
共通鍵で復号する
S122
ディスク鍵を取得する
S123
ブロック鍵を生成する
S124
リターン

図17

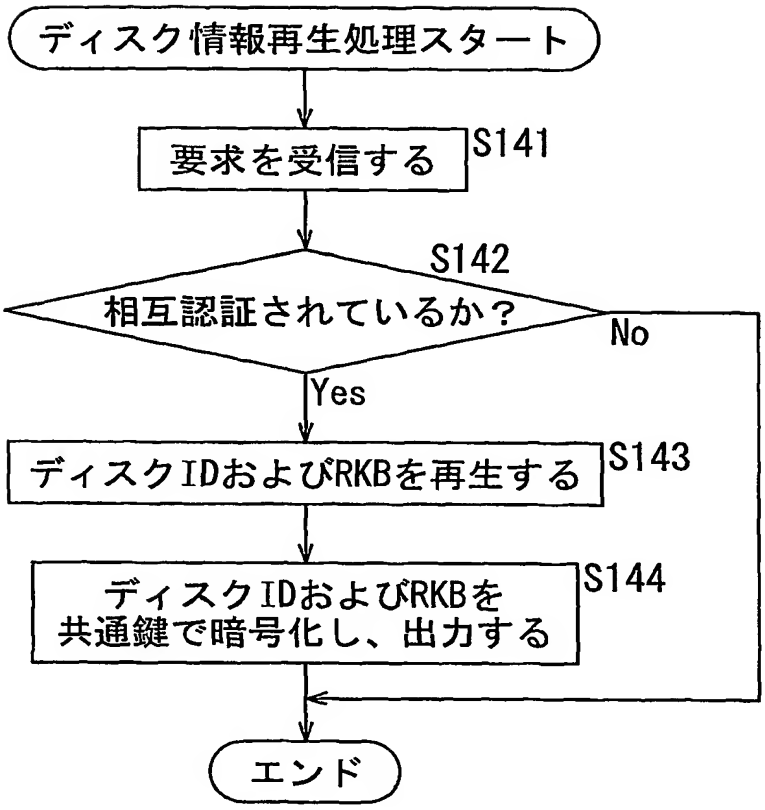

ディスク情報再生処理スタート
要求を受信する
S141
S142
相互認証されているか？
No
Yes
ディスクIDおよびRKBを再生する
S143
ディスクIDおよびRKBを
共通鍵で暗号化し、出力する
S144
エンド

図18

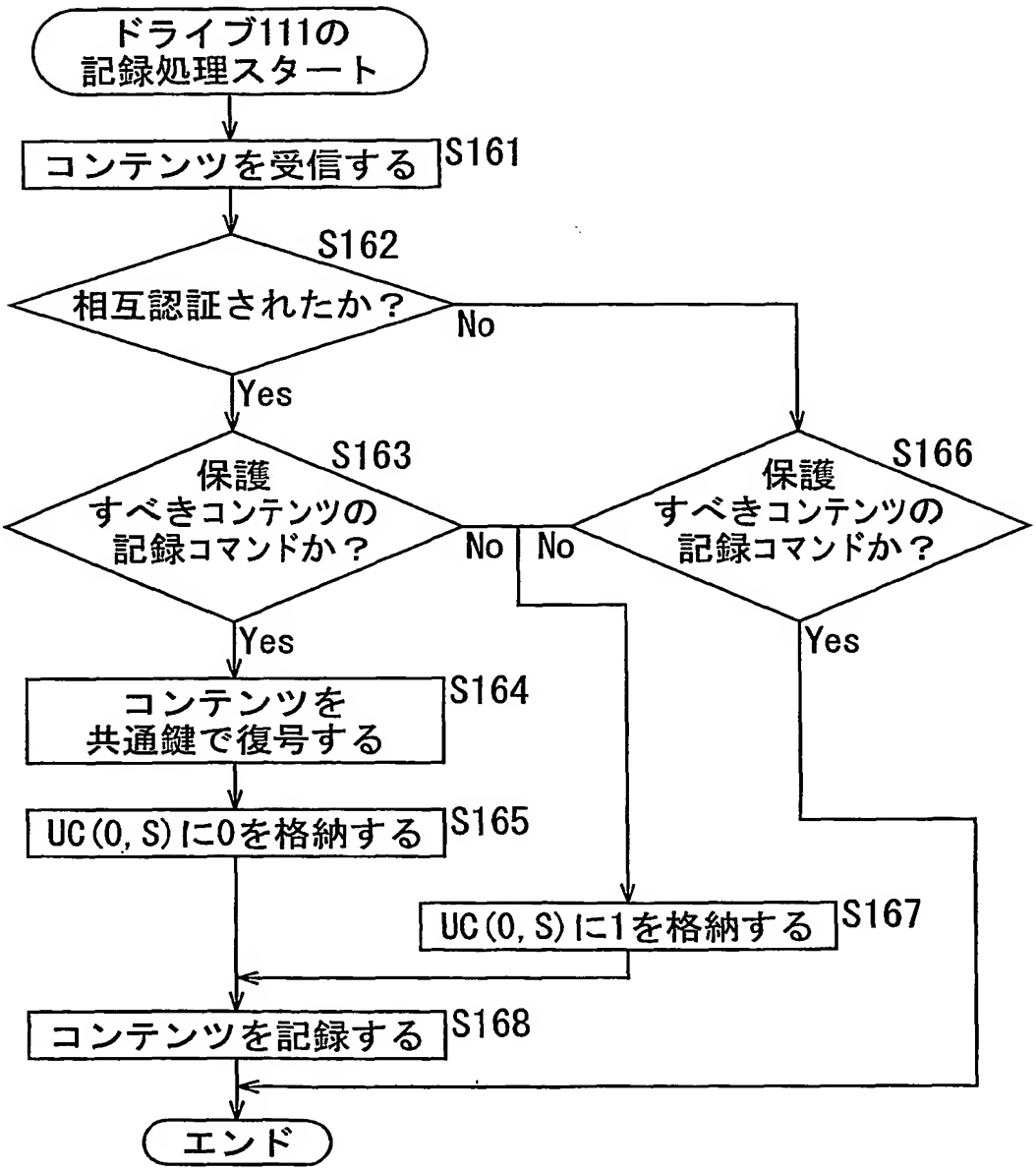

ドライブ111の
記録処理スタート
コンテンツを受信する
S161
S162
相互認証されたか？
No
Yes
S163
保護
すべきコンテンツの
記録コマンドか？
No
S166
保護
すべきコンテンツの
記録コマンドか？
No
Yes
Yes
コンテンツを
共通鍵で復号する
S164
UC(0, S)に0を格納する
S165
UC(0, S)に1を格納する
S167
コンテンツを記録する
S168
エンド

図19

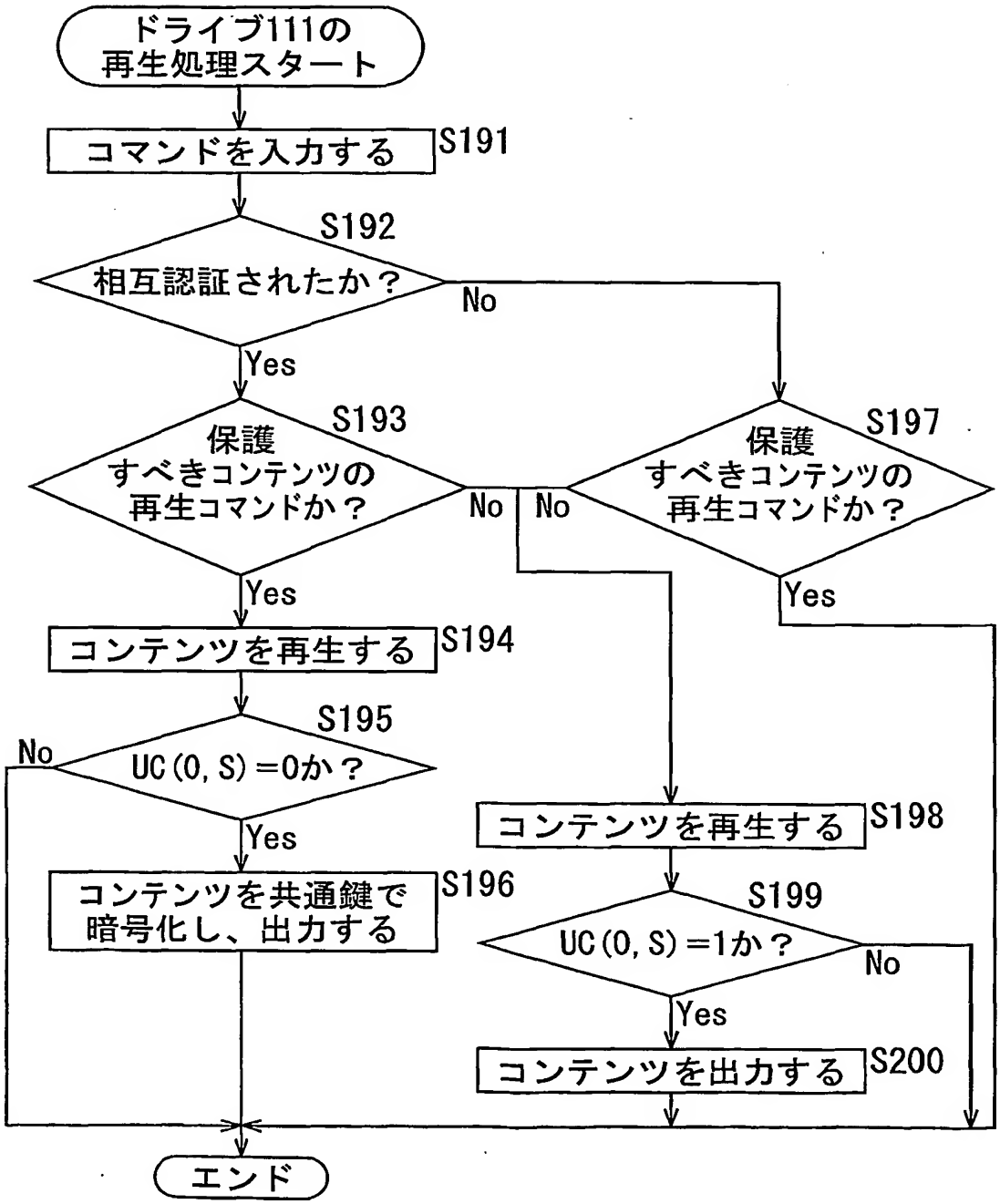

ドライブ111の
再生処理スタート
コマンドを入力する
S191
S192
相互認証されたか？
No
Yes
S193
保護
すべきコンテンツの
再生コマンドか？
No
Yes
S197
保護
すべきコンテンツの
再生コマンドか？
No
Yes
コンテンツを再生する
S194
S195
No
UC(0, S)＝0か？
Yes
コンテンツを共通鍵で
暗号化し、出力する
S196
コンテンツを再生する
S198
S199
UC(0, S)＝1か？
No
Yes
コンテンツを出力する
S200
エンド

図20

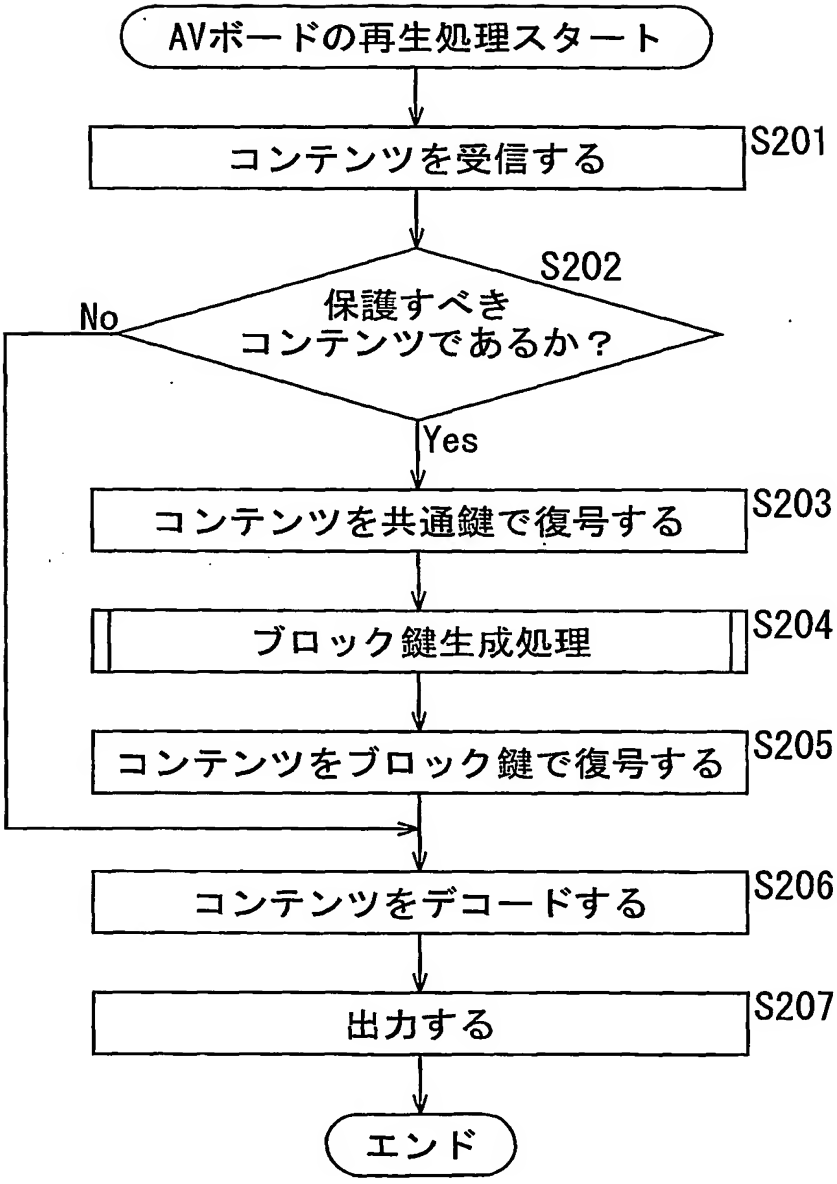

AVボードの再生処理スタート
コンテンツを受信する
S201
S202
保護すべき
コンテンツであるか？
No
Yes
コンテンツを共通鍵で復号する
S203
ブロック鍵生成処理
S204
コンテンツをブロック鍵で復号する
S205
コンテンツをデコードする
S206
出力する
S207
エンド

図21

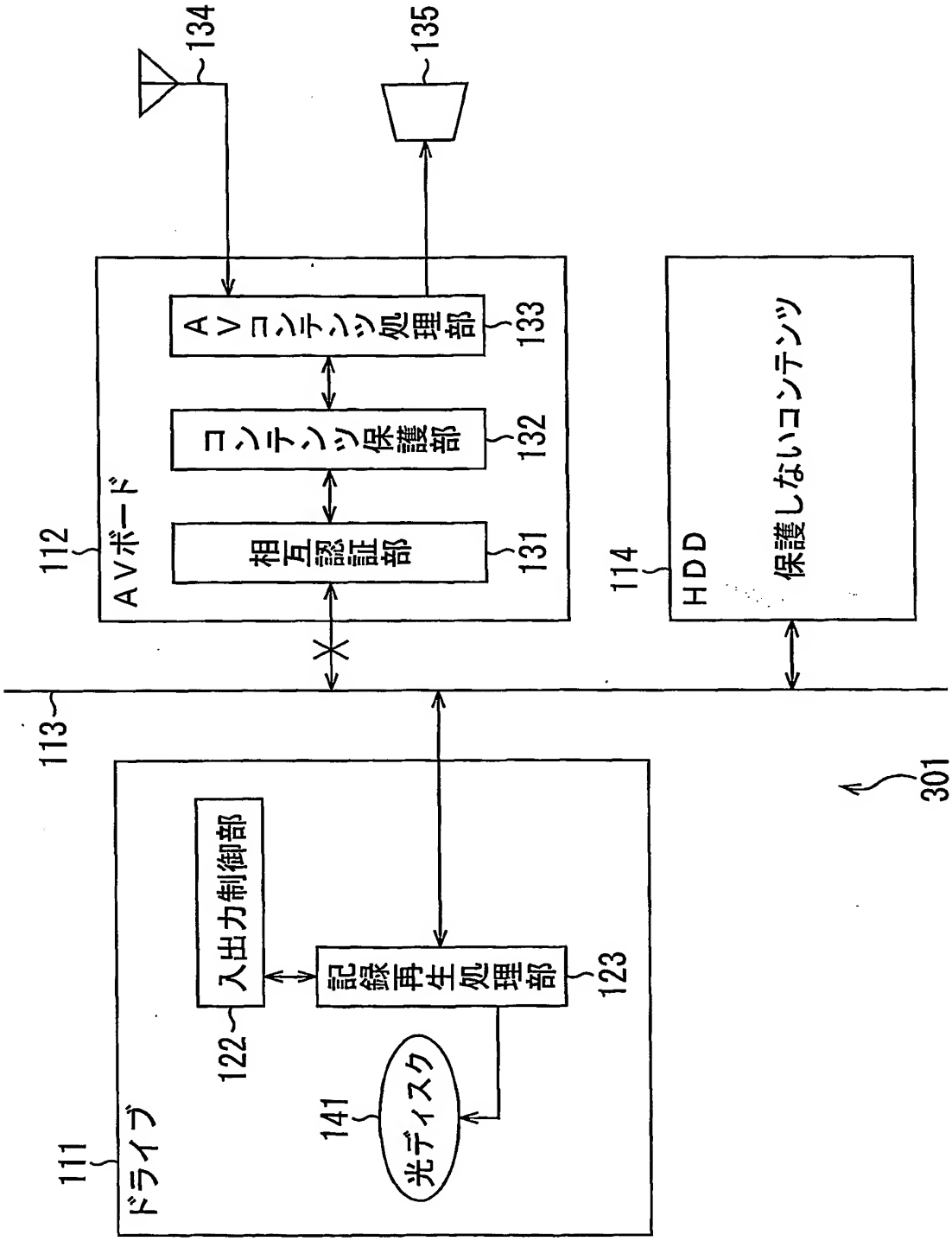

134
135
AVコンテンツ処理部
133
コンテンツ保護部
132
相互認証部
131
112
AVボード
114
HDD
保護しないコンテンツ
113
301
入出力制御部
122
記録再生処理部
123
141
光ディスク
111
ドライブ

図22

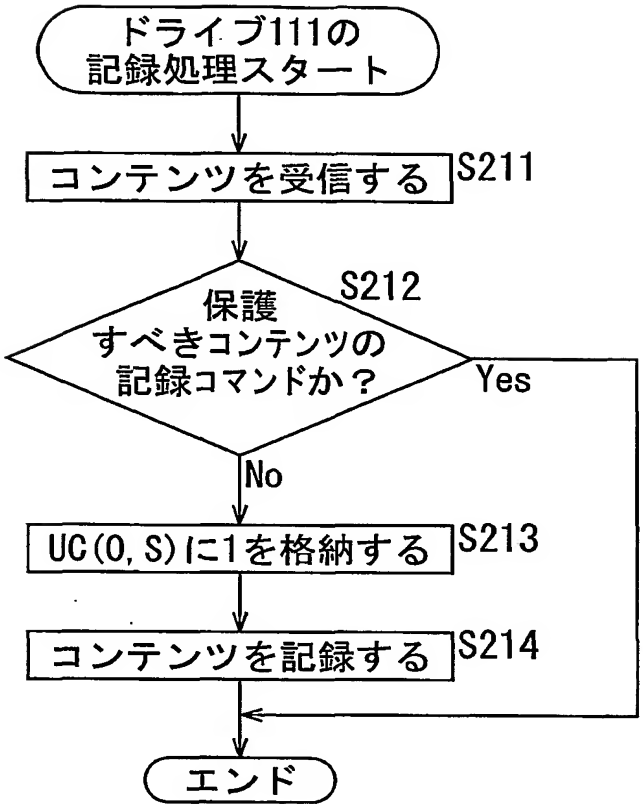

ドライブ111の
記録処理スタート
コンテンツを受信する
S211
S212
保護
すべきコンテンツの
記録コマンドか？
Yes
No
UC(0, S)に1を格納する
S213
コンテンツを記録する
S214
エンド

図23

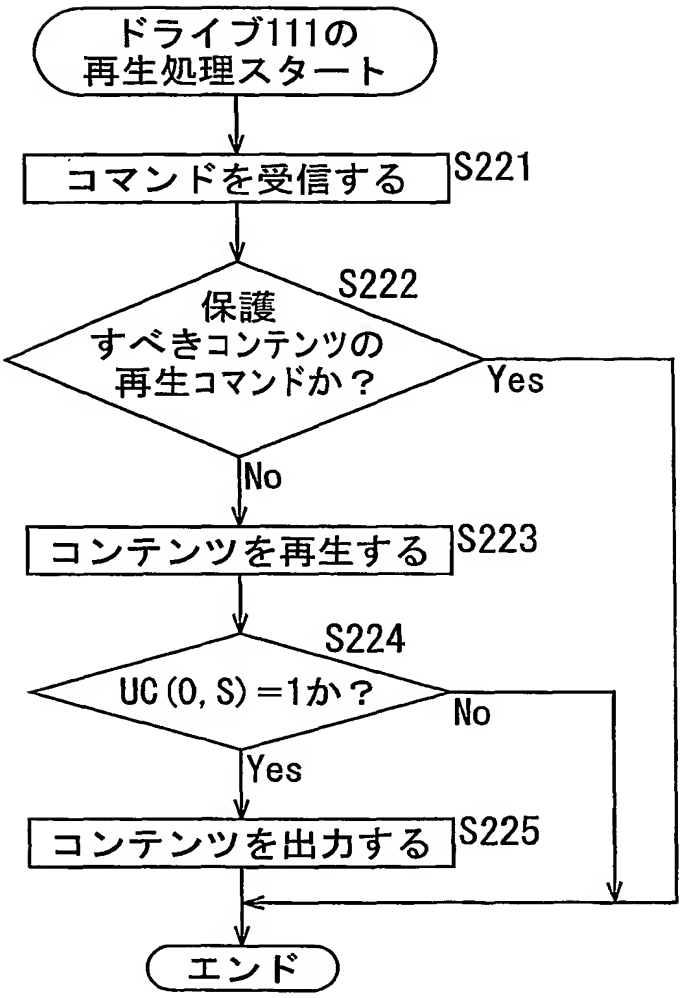

ドライブ111の
再生処理スタート
コマンドを受信する
S221
S222
保護
すべきコンテンツの
再生コマンドか？
Yes
No
コンテンツを再生する
S223
S224
UC(0, S)＝1か？
No
Yes
コンテンツを出力する
S225
エンド

図24

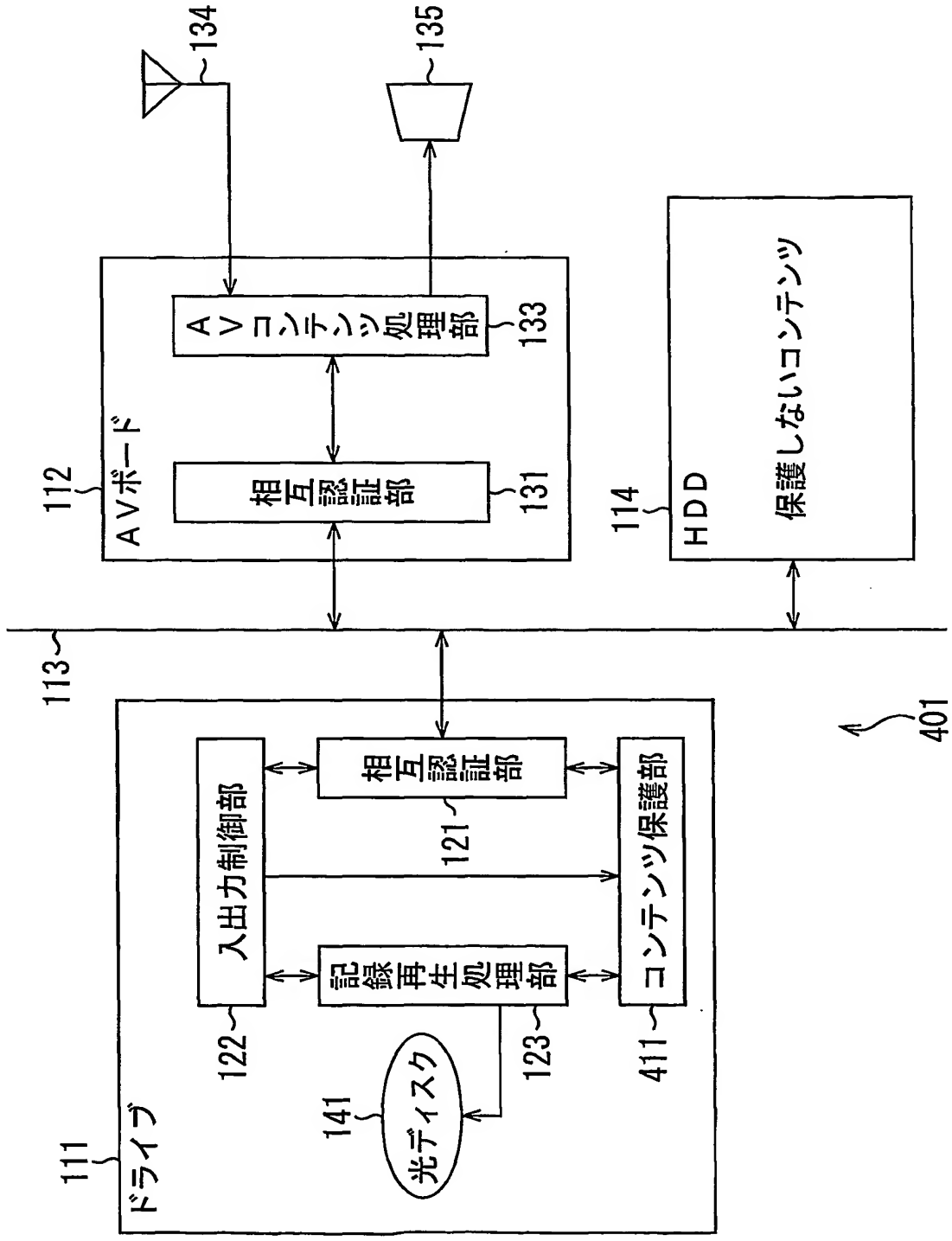

134
135
AVコンテンツ処理部
133
112
AVボード
相互認証部
131
114
HDD
保護しないコンテンツ
113
401
相互認証部
121
入出力制御部
122
記録再生処理部
123
コンテンツ保護部
411
141
光ディスク
111
ドライブ

図25

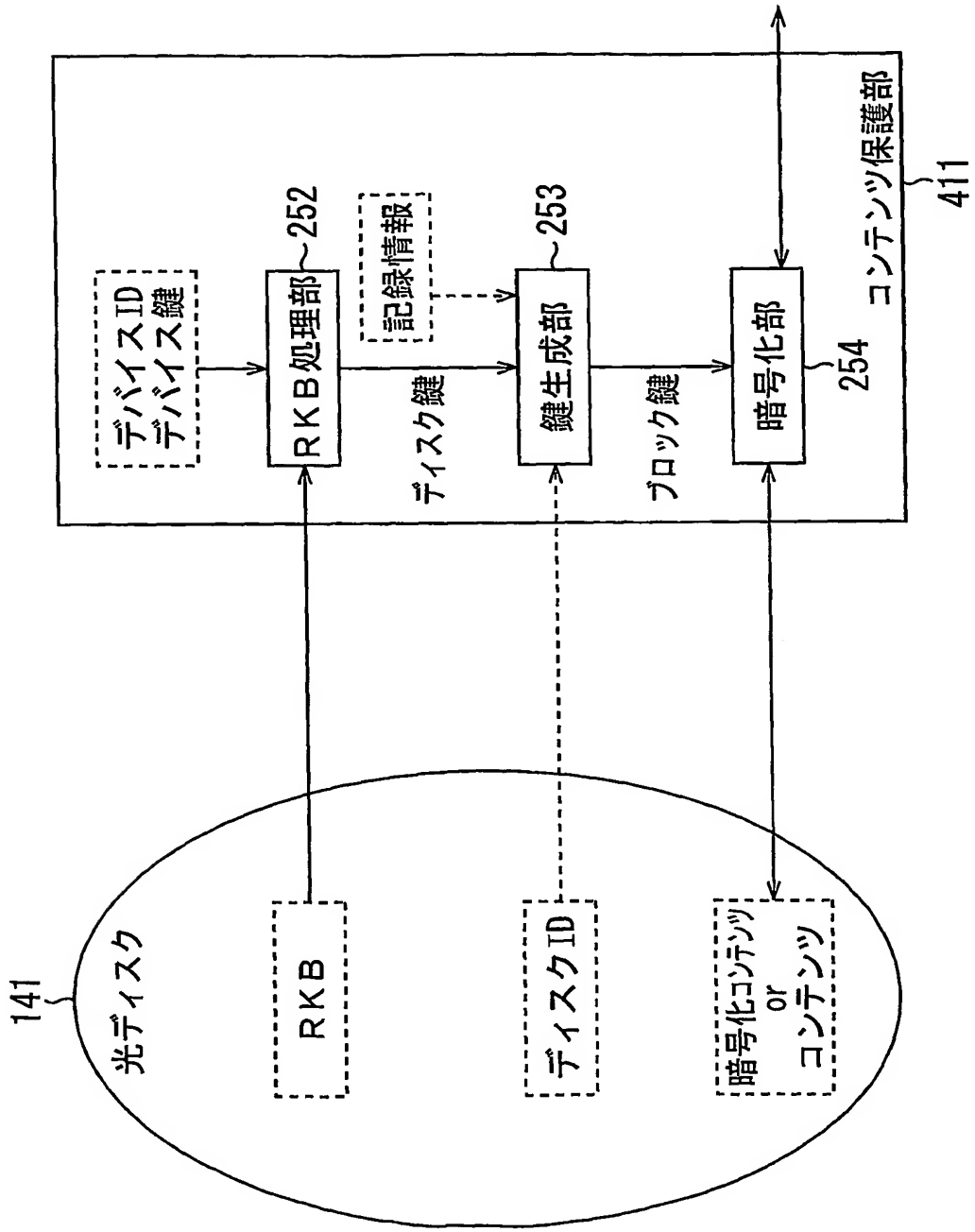

141
光ディスク
RKB
ディスクID
暗号化コンテンツ
or
コンテンツ
デバイスID
デバイス鍵
RKB処理部
252
記録情報
ディスク鍵
鍵生成部
253
ブロック鍵
暗号化部
254
コンテンツ保護部
411

図26

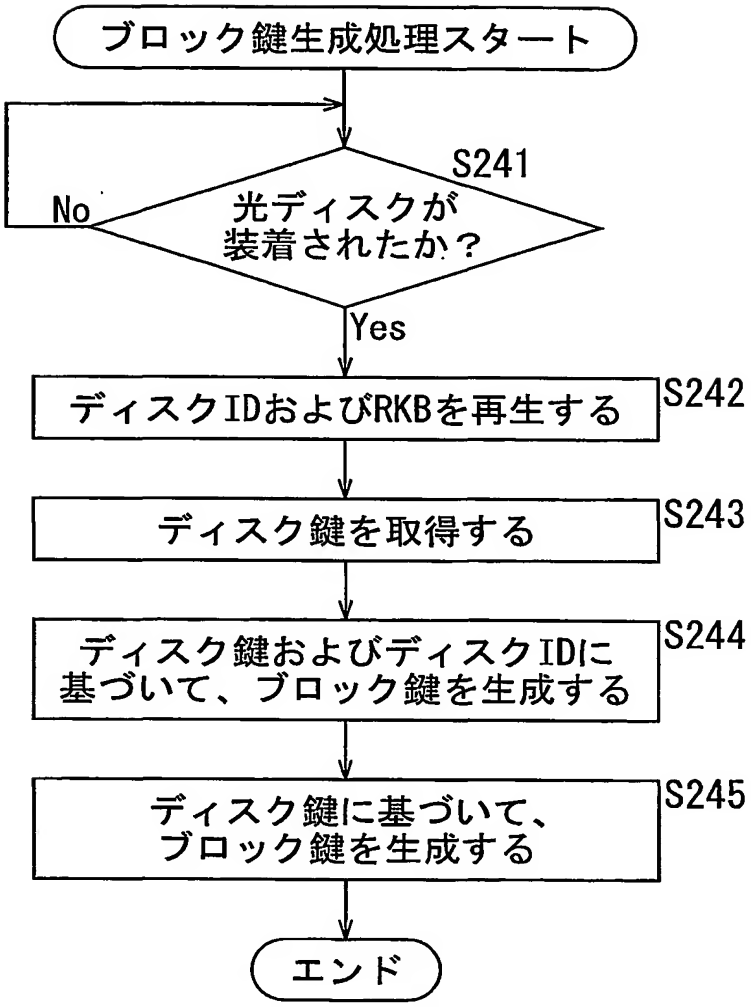

ブロック鍵生成処理スタート
S241
No
光ディスクが
装着されたか？
Yes
ディスクIDおよびRKBを再生する
S242
ディスク鍵を取得する
S243
ディスク鍵およびディスクIDに
基づいて、ブロック鍵を生成する
S244
ディスク鍵に基づいて、
ブロック鍵を生成する
S245
エンド

図27

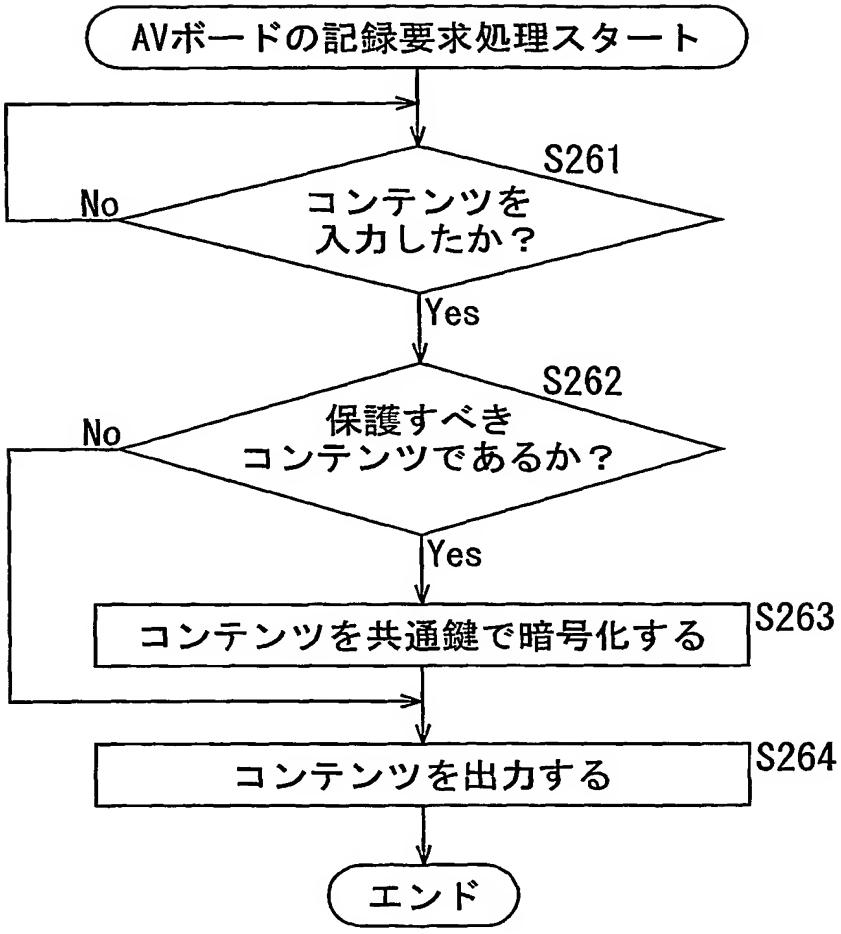

AVボードの記録要求処理スタート
S261
コンテンツを
入力したか？
No
Yes
S262
保護すべき
コンテンツであるか？
No
Yes
コンテンツを共通鍵で暗号化する
S263
コンテンツを出力する
S264
エンド

図28

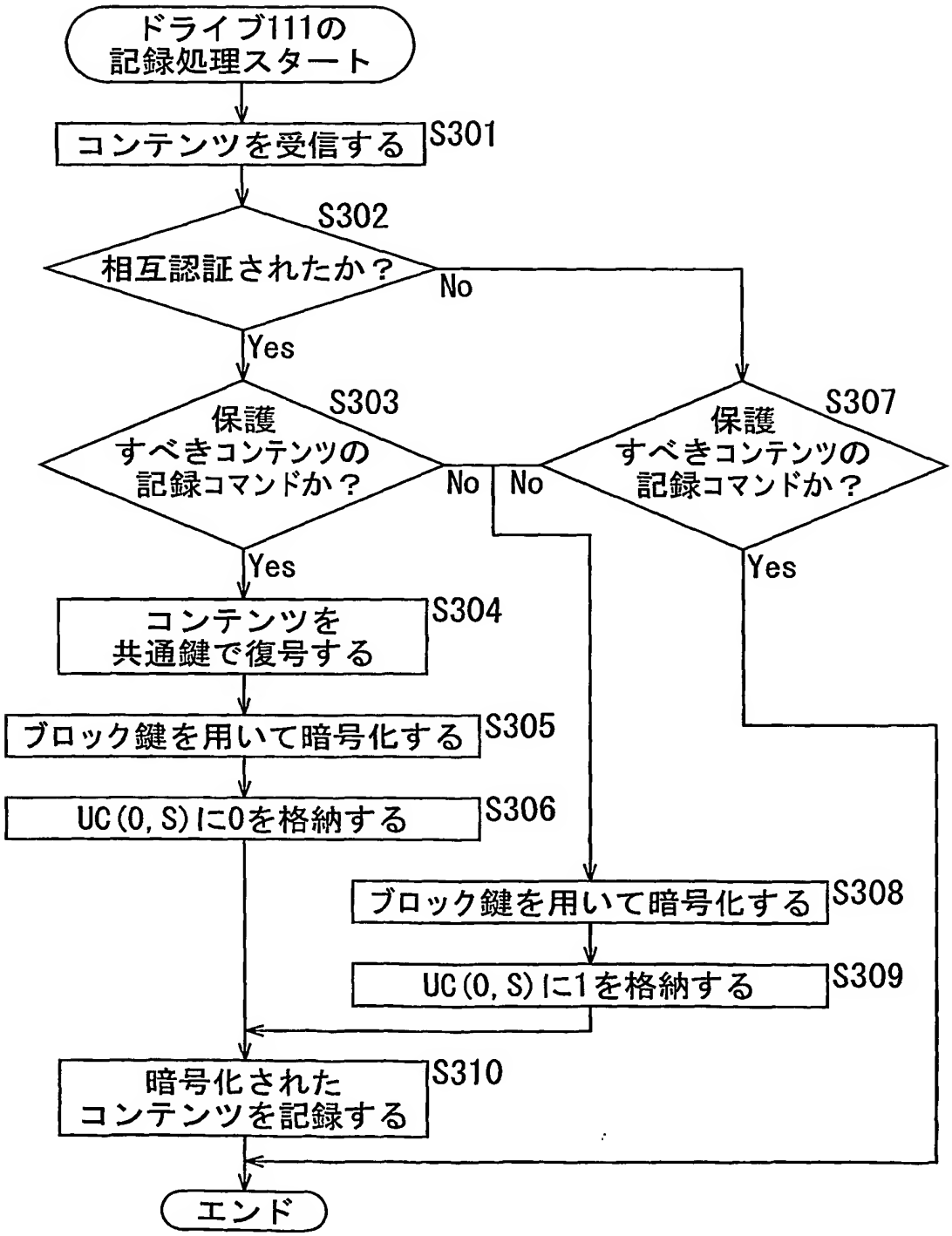

ドライブ111の
記録処理スタート
コンテンツを受信する
S301
S302
相互認証されたか？
No
Yes
S303
保護
すべきコンテンツの
記録コマンドか？
No
Yes
S304
コンテンツを
共通鍵で復号する
ブロック鍵を用いて暗号化する
S305
UC(0, S)に0を格納する
S306
S307
保護
すべきコンテンツの
記録コマンドか？
No
Yes
ブロック鍵を用いて暗号化する
S308
UC(0, S)に1を格納する
S309
暗号化された
コンテンツを記録する
S310
エンド

図29

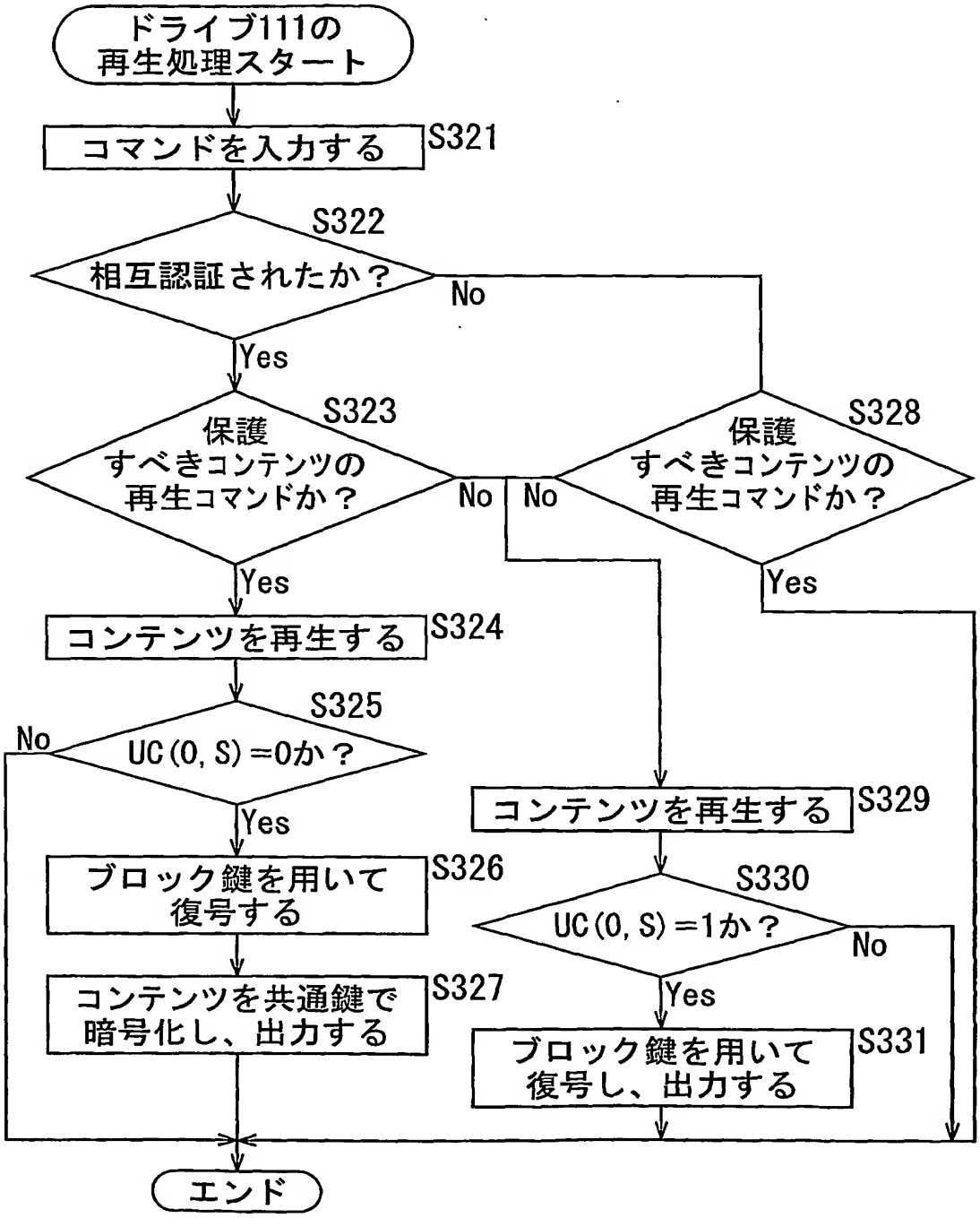

ドライブ111の
再生処理スタート
コマンドを入力する
S321
S322
相互認証されたか？
No
Yes
S323
保護
すべきコンテンツの
再生コマンドか？
No
Yes
S328
保護
すべきコンテンツの
再生コマンドか？
No
Yes
コンテンツを再生する
S324
S325
No
UC(0, S)＝0か？
Yes
ブロック鍵を用いて
復号する
S326
コンテンツを共通鍵で
暗号化し、出力する
S327
コンテンツを再生する
S329
S330
UC(0, S)＝1か？
No
Yes
ブロック鍵を用いて
復号し、出力する
S331
エンド

図30

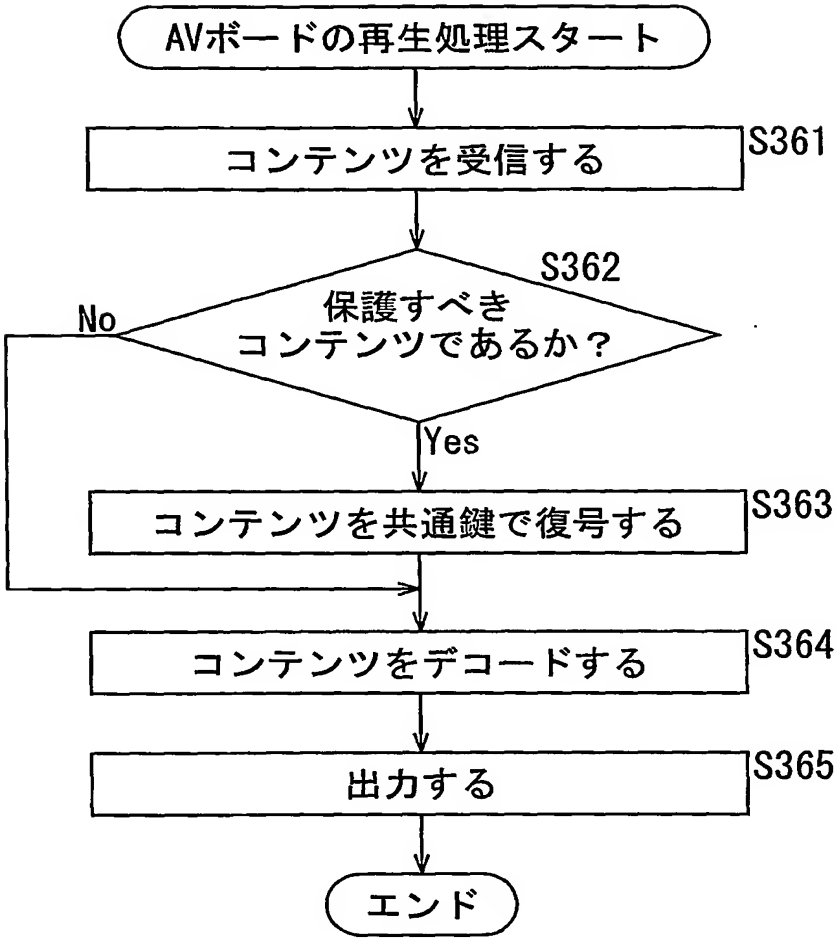

AVボードの再生処理スタート
コンテンツを受信する
S361
S362
保護すべき
コンテンツであるか？
No
Yes
コンテンツを共通鍵で復号する
S363
コンテンツをデコードする
S364
出力する
S365
エンド

図31

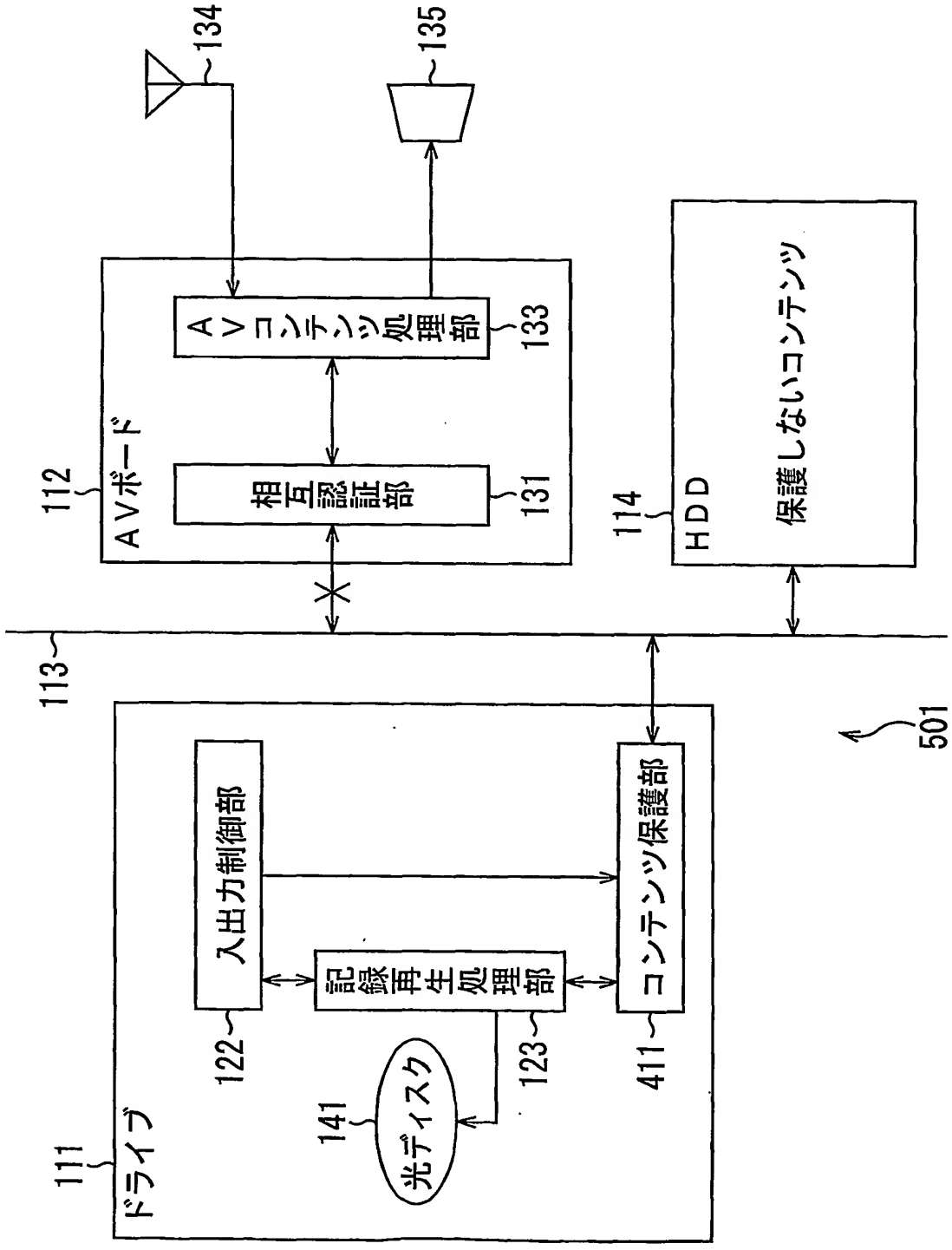

134
135
AVコンテンツ処理部
133
112
AVボード
相互認証部
131
114
HDD
保護しないコンテンツ
113
501
入出力制御部
122
記録再生処理部
123
コンテンツ保護部
411
141
光ディスク
111
ドライブ

図32

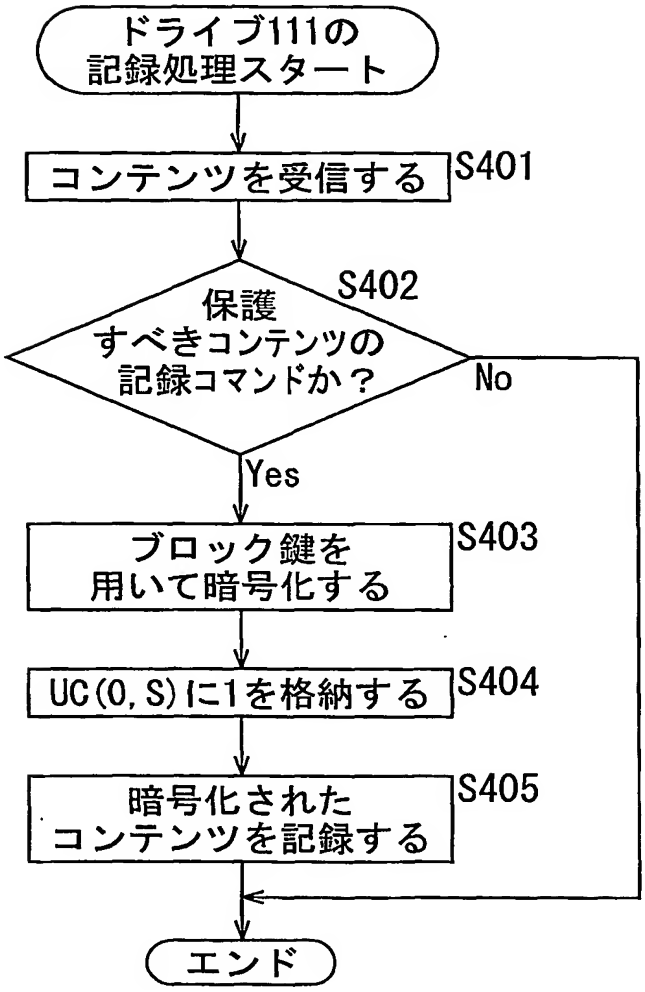

ドライブ111の
記録処理スタート
コンテンツを受信する
S401
保護
すべきコンテンツの
記録コマンドか？
S402
No
Yes
ブロック鍵を
用いて暗号化する
S403
UC(0, S)に1を格納する
S404
暗号化された
コンテンツを記録する
S405
エンド

図33

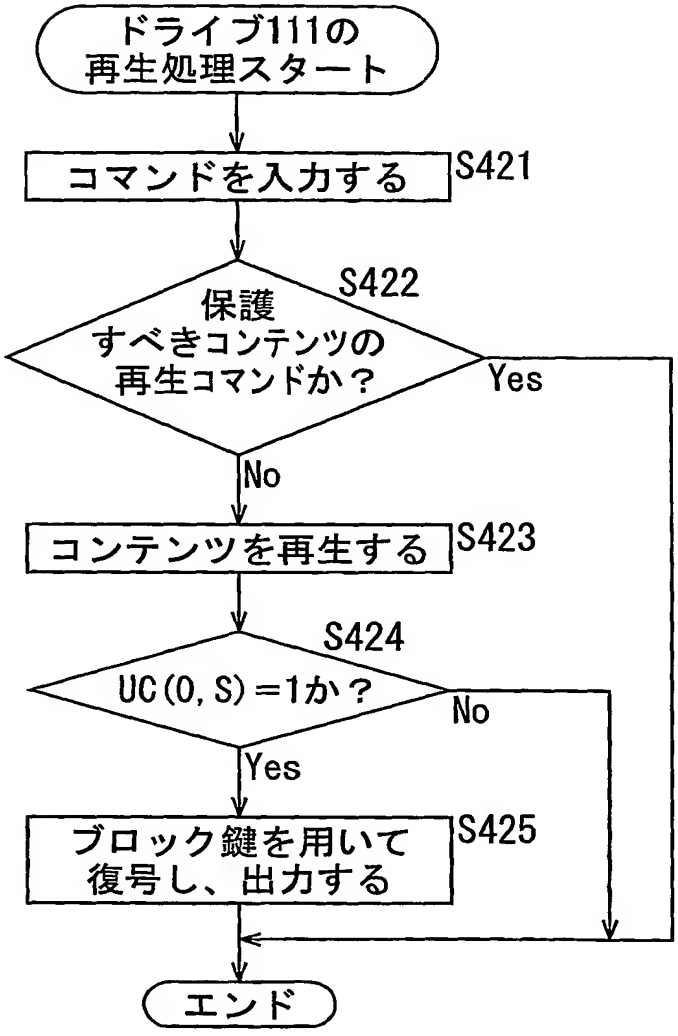
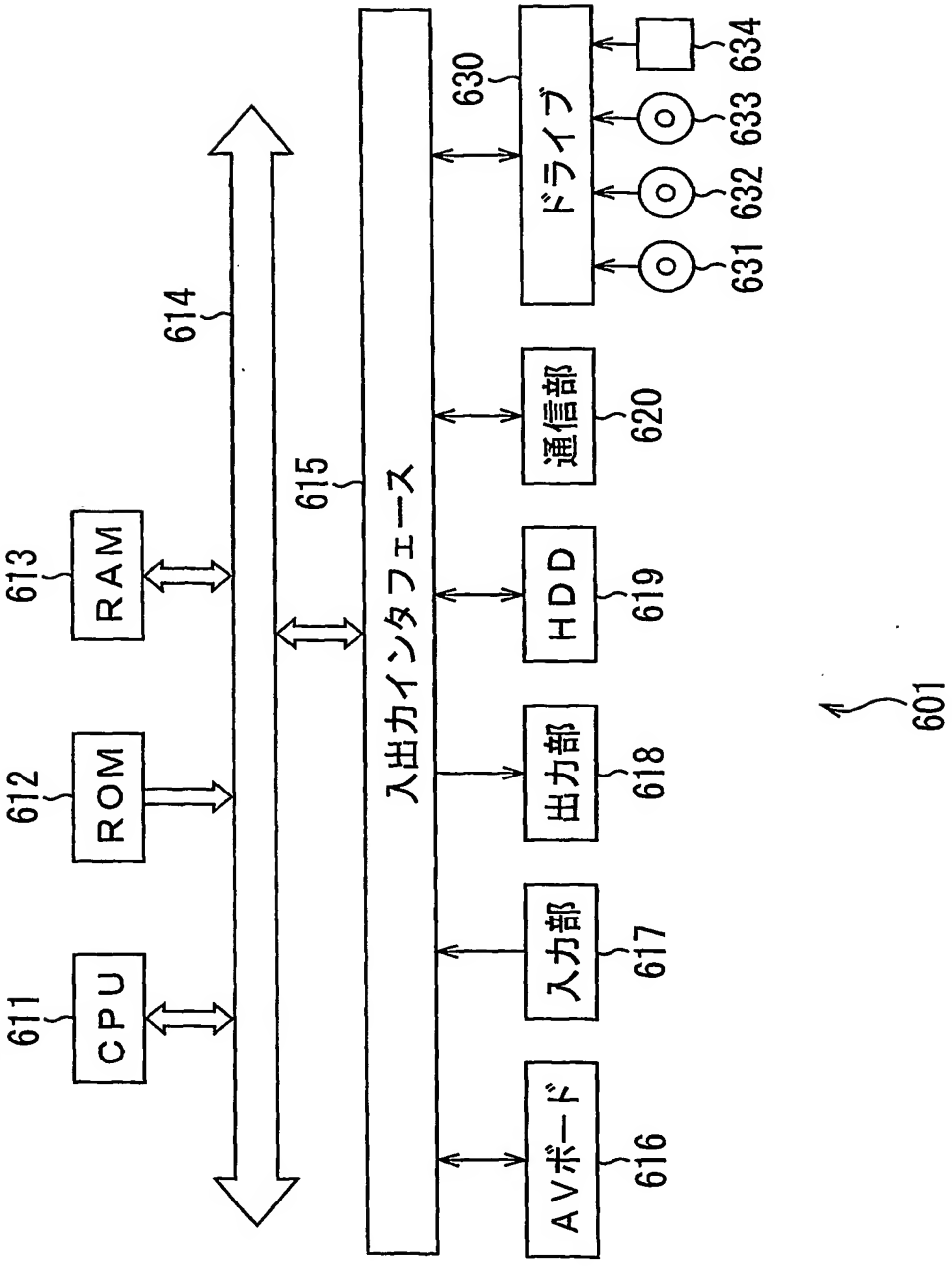

ドライブ111の
再生処理スタート
コマンドを入力する
S421
S422
保護
すべきコンテンツの
再生コマンドか？
Yes
No
コンテンツを再生する
S423
S424
UC(0, S)＝1か？
No
Yes
ブロック鍵を用いて
復号し、出力する
S425
エンド

図34


CPU
611
ROM
612
RAM
613
614
615
入出力インタフェース
AVボード
616
入力部
617
出力部
618
HDD
619
通信部
620
ドライブ
630
631
632
633
634
601

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/13752

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/14, G09C1/00, G11B20/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/14, G09C1/00, G11B20/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho	1922-1996	Toroku Jitsuyo Shinan Koho	1994-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Jitsuyo Shinan Toroku Koho	1996-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	JP 2000-285027 A (Matsushita Electric Industrial Co., Ltd.), 13 October, 2000 (13.10.00),	1-3,8,9, 23-26,31-34, 37-39
Y	All pages; all drawings; particularly, Claim 8 & WO 00/26910 A1 & EP 1045389 A1	4-7,10-22, 27-30,35,36
Y	JP 2002-84271 A (Sony Corp.), 22 March, 2002 (22.03.02.), All pages; all drawings & EP 1187391 A2	4,5,7,11,12, 18,19,29
Y	"5C Digital Transmission Content Protection White Paper", [online], 14 July, 1998 (14.07.98), DTLA, [retrieved on 08 January, 2004 (08.01.04)], Retrieved from the Internet: <URL: http://www.dtcp.com/data/wp_spec.pdf>	6,10-22, 27-30,35,36

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search 08 January, 2004 (08.01.04)	Date of mailing of the international search report 27 January, 2004 (27.01.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP03/13752

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2002-132457 A (Victor Company Of Japan, Ltd.), 10 May, 2002 (10.05.02), All pages; all drawings; particularly, Par. No. [0068] (Family: none)	1-39
A	JP 2000-187935 A (Matsushita Electric Industrial Co., Ltd.), 04 July, 2000 (04,07.00), All pages; all drawings; particularly, Par. No. [0019] & WO 00/05716 A1 & EP 1018733 A1	1-39
A	JP 11-306677 A (Sony Corp.), 05 November, 1999 (05.11.99), All pages; all drawings & EP 938091 A2	1-39

国際調査報告	国際出願番号　ＰＣＴ／ＪＰ０３／１３７５２

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））
Int.Cl.[7]　G06F12/14, G09C1/00, G11B20/10

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））
Int.Cl.[7]　G06F12/14, G09C1/00, G11B20/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922 - 1996 年
日本国公開実用新案公報	1971 - 2004 年
日本国登録実用新案公報	1994 - 2004 年
日本国実用新案登録公報	1996 - 2004 年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
X	JP 2000-285027 A (松下電器産業株式会社) 2000.10.13, 全頁, 全図, 特に【請求項８】 & WO 00/26910 A1 & EP 1045389 A1	1-3, 8, 9, 23-26, 31-34, 37-39
Y		4-7, 10-22, 27-30, 35, 36
Y	JP 2002-84271 A (ソニー株式会社) 2002.03.22, 全頁, 全図 & EP 1187391 A2	4, 5, 7, 11, 12, 18, 19, 29

☒ Ｃ欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
08.01.2004	27.1.2004

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	奥村　元宏	５Ｎ　３０４４
	電話番号　０３－３５８１－１１０１　内線　３５８５	

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（１９９８年７月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	"5C Digital Transmission Content Protection White Paper", [online], 1998.07.14, DTLA, [retrieved on 2004-01-08], Retrieved from the Internet: <URL: http://www.dtcp.com/data/wp_spec.pdf>	6,10-22, 27-30,35,36
A	JP 2002-132457 A (日本ビクター株式会社) 2002.05.10, 全頁, 全図, 特に【００６８】段落 (ファミリーなし)	1-39
A	JP 2000-187935 A (松下電器産業株式会社) 2000.07.04, 全頁, 全図, 特に【００１９】段落 & WO 00/05716 A1 & EP 1018733 A1	1-39
A	JP 11-306677 A (ソニー株式会社) 1999.11.05, 全頁, 全図 & EP 938091 A2	1-39